UNITED STATES DISTRICT COURT FOR THE
EASTERN DISTRICT OF PENNSYLVANIA

COMCAST CABLE COMMUNICATIONS, LLC; TVWORKS, LLC; and COMCAST MO GROUP, INC., Plaintiffs, v. SPRINT COMMUNICATIONS COMPANY L.P.; SPRINT SPECTRUM L.P.; and NEXTEL OPERATIONS, INC., Defendants.	Civil Action No.: 2:12-cv-00859-JD DEMAND FOR JURY TRIAL

FIRST AMENDED COMPLAINT FOR PATENT INFRINGEMENT

Plaintiffs Comcast Cable Communications, LLC ("Comcast Cable Communications"), TVWorks, LLC ("TVWorks"), and Comcast MO Group, Inc. ("Comcast MO Group") (collectively, "Comcast"), for their First Amended Complaint for patent infringement against Defendants Sprint Communications Company L.P. ("Sprint Communications"), Sprint Spectrum L.P. ("Sprint Spectrum"), and Nextel Operations, Inc. ("Nextel") (collectively, "Sprint"), allege as follows:

THE PARTIES

1. Plaintiff Comcast Cable Communications is a limited liability company organized under the laws of the State of Delaware, with its principal place of business in Philadelphia, Pennsylvania. Comcast Cable Communications is a wholly owned, indirect subsidiary of Comcast Corporation, the principal place of business of which is also in Philadelphia, Pennsylvania.

2. Plaintiff TVWorks is a limited liability company organized under the laws of the State of Delaware, with its principal place of business in Philadelphia,

Pennsylvania. TVWorks is a wholly owned subsidiary of Comcast Cable Communications.

3. Plaintiff Comcast MO Group is a corporation organized under the laws of the State of Delaware, with its principal place of business in Philadelphia, Pennsylvania. Comcast MO Group is a wholly owned, indirect subsidiary of Comcast Corporation.

4. Defendant Sprint Communications is a limited partnership organized under the laws of the State of Delaware, with its principal place of business in Overland Park, Kansas. On information and belief, Sprint Communications is a wholly owned subsidiary of Sprint Nextel Corporation.

5. Defendant Sprint Spectrum is a limited partnership organized under the laws of the State of Delaware, with its principal place of business in Overland Park, Kansas. On information and belief, Sprint Spectrum is a wholly owned subsidiary of Sprint Nextel Corporation.

6. Defendant Nextel Operations is a corporation organized under the laws of the State of Delaware, with its principal place of business in Overland Park, Kansas. On information and belief, Nextel Operations is a wholly owned subsidiary of Sprint Nextel Corporation.

JURISDICTION AND VENUE

7. This action arises under the United States patent laws, 35 U.S.C. §§ 101, *et seq.* The Court has subject matter jurisdiction over this action pursuant to 28 U.S.C. §§ 1331 and 1338(a).

8. The Court has personal jurisdiction over Sprint because Sprint transacts business within the judicial district and has committed acts of patent infringement within the judicial district.

9. Venue is proper in this district pursuant to 28 U.S.C. §§ 1391(b)-(c) and 1400(b).

FIRST CAUSE OF ACTION
(SPRINT'S INFRINGEMENT OF U.S. PATENT NO. 6,885,870)

10. Comcast restates and realleges the allegations set forth in paragraphs 1 through 9 above and incorporates them by reference.

11. Comcast Cable Communications is the lawful owner, by assignment, of the entire right, title, and interest in United States Patent No. 6,885,870 ("the '870 patent"), entitled "Transferring Of A Message," which was issued on April 26, 2005 to inventor Outi Aho. On October 4, 2011, the United States Patent and Trademark Office issued an *ex parte* reexamination certificate adding 93 new claims to the '870 patent. A copy of the '870 patent, the reexamination certificate, and a certificate of correction issued on March 13, 2012 is attached hereto as Exhibit A.

12. Sprint has been and now is infringing the '870 patent, within this judicial district and elsewhere, by making, using, offering for sale, and/or selling products and services that transfer a message. Such products and services include, without limitation, Sprint's MMS products and services for wireless (such as, for example, Sprint Wireless Picture Mail, Sprint Wireless Video Mail, and Sprint Mobile Email).

13. Comcast Cable Communications has been damaged by Sprint's infringement of the '870 patent, has been irreparably harmed by that infringement, and will suffer additional damages and irreparable harm unless this Court enjoins Sprint from further infringement.

SECOND CAUSE OF ACTION
(SPRINT'S INFRINGEMENT OF U.S. PATENT NO. 5,987,323)

14. Comcast restates and realleges the allegations set forth in paragraphs 1 through 13 above and incorporates them by reference.

15. Comcast Cable Communications is the lawful owner, by assignment, of the entire right, title, and interest in United States Patent No. 5,987,323 ("the '323 patent"), entitled "Starting A Short Message Transmission In A Cellular Communication System," which was issued on November 16, 1999 to inventor Seppo Huotari. A copy of the '323 patent is attached hereto as Exhibit B.

16. Sprint has been and now is infringing the '323 patent, within this judicial district and elsewhere, by making, using, offering for sale, and/or selling products and services that start a short message transmission in a cellular communications system. Such products and services include, without limitation, Sprint's SMS products and services for wireless (such as, for example, services currently or previously provided under its Vision Pack, Unlimited Texting, Wireless Texting, and Wireless Premium Text Message plans) and Sprint's MMS products and services for wireless (such as, for example, Sprint Wireless Picture Mail, Sprint Wireless Video Mail, and Sprint Mobile Email).

17. Comcast Cable Communications has been damaged by Sprint's infringement of the '323 patent, has been irreparably harmed by that infringement, and will suffer additional damages and irreparable harm unless this Court enjoins Sprint from further infringement.

THIRD CAUSE OF ACTION
(SPRINT'S INFRINGEMENT OF U.S. PATENT NO. 6,112,305)

18. Comcast restates and realleges the allegations set forth in paragraphs 1 through 17 above and incorporates them by reference.

19. TVWorks is the lawful owner, by assignment, of the entire right, title, and interest in United States Patent No. 6,112,305 ("the '305 patent"), entitled "Mechanism For Dynamically Binding A Network Computer Client Device To An Approved Internet

Service Provider," which was issued on August 29, 2000 to inventors Frank Dancs and James Zmuda. A copy of the '305 patent is attached hereto as Exhibit C.

20. Sprint has been and now is infringing the '305 patent, within this judicial district and elsewhere, by making, using, offering for sale, and/or selling products and services that connect a network computer client device to an approved internet service provider. Such products and services include, without limitation, Sprint's wireless data products and services (such as, for example, services currently or previously provided by Sprint Mobile Broadband USB modems and PCMCIA wireless cards or under Sprint's 3G Mobile Broadband Connection and Power Vision plans).

21. TVWorks has been damaged by Sprint's infringement of the '305 patent, has been irreparably harmed by that infringement, and will suffer additional damages and irreparable harm unless this Court enjoins Sprint from further infringement.

FOURTH CAUSE OF ACTION
(SPRINT'S INFRINGEMENT OF U.S. PATENT NO. 5,991,271)

22. Comcast restates and realleges the allegations set forth in paragraphs 1 through 21 above and incorporates them by reference.

23. Comcast MO Group is the lawful owner, by assignment, of the entire right, title, and interest in United States Patent No. 5,991,271 ("the '271 patent"), entitled "Signal-To-Channel Mapping For Multi-Channel, Multi-Signal Transmission Systems," which was issued on November 23, 1999 to inventors David Jones, Youngho Lee, and Bruce Phillips. A copy of the '271 patent is attached hereto as Exhibit D.

24. Sprint has been and now is infringing the '271 patent, within this judicial district and elsewhere, by making, using, offering for sale, and/or selling products and services that perform signal-to-channel mapping for multi-channel, multi-signal transmission systems. Such products and services include, without limitation, Sprint's

MPLS/GMPLS networks and its optical networks using reconfigurable optical add-drop multiplexers.

25. Comcast MO Group has been damaged by Sprint's infringement of the '271 patent, has been irreparably harmed by that infringement, and will suffer additional damages and irreparable harm unless this Court enjoins Sprint from further infringement.

PRAYER FOR RELIEF

WHEREFORE, Comcast prays for judgment:

1. that Sprint has infringed and is infringing the '870 patent, the '323 patent, the '305 patent, and the '271 patent;

2. enjoining Sprint, its officers, agents, servants, employees, attorneys and all other persons in active concert or participation with any of them from infringing the '870 patent, the '323 patent, the '305 patent, and the '271 patent;

3. awarding Comcast compensatory damages for Sprint's infringement, together with interest and costs pursuant to 35 U.S.C. § 284;

4. awarding Comcast reasonable attorneys' fees pursuant to 35 U.S.C. § 285; and

5. granting Comcast such other and further relief in law or in equity as this Court deems just or proper.

DEMAND FOR JURY TRIAL

Comcast demands a trial by jury on all issues so triable.

Dated: June 6, 2012

HANGLEY ARONCHICK SEGAL PUDLIN & SCHILLER

By: _____

William T. Hangley (I.D. No. 03533)
Michael Lieberman (I.D. No. 62425)
Rebecca L. Santoro (I.D. No. 206210)
One Logan Square, 27th Floor
Philadelphia, PA 19103
Telephone: (215) 496-7374

DAVIS POLK & WARDWELL LLP

Matthew B. Lehr (*pro hac vice*)
Anthony Fenwick (*pro hac vice*)
David J. Lisson (*pro hac vice*)
Austin D. Tarango (*pro hac vice*)
Shiwoong Kim (*pro hac vice*)
1600 El Camino Real
Menlo Park, CA 94025
Telephone: (650) 752-2000
Facsimile: (650) 752-2111

Attorneys for Plaintiffs Comcast Cable Communications, LLC, TVWorks, LLC, and Comcast MO Group, Inc.

EXHIBIT A

US006885870B2

(12) **United States Patent**
Aho

(10) **Patent No.: US 6,885,870 B2**
(45) **Date of Patent: Apr. 26, 2005**

(54) **TRANSFERRING OF A MESSAGE**

(75) Inventor: **Outi Aho**, Lempäälä (FI)

(73) Assignee: **Nokia Mobile Phones, Ltd.**, Espoo (FI)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 849 days.

(21) Appl. No.: **09/745,756**

(22) Filed: **Feb. 22, 2001**

(65) **Prior Publication Data**

US 2001/0005675 A1 Jun. 28, 2001

(30) **Foreign Application Priority Data**

Dec. 23, 1999 (FI) 19992783

(51) **Int. Cl.**[7] **H04Q 7/20**
(52) **U.S. Cl.** **455/466**; 455/432.3; 455/432.1; 370/353; 370/395.1
(58) **Field of Search** 455/509, 510, 455/515, 466, 552.1, 556.1, 557; 370/352, 353, 395.1, 395.2

(56) **References Cited**

U.S. PATENT DOCUMENTS

5,878,347 A 3/1999 Joensuu et al. 455/433
5,920,820 A 7/1999 Qureshi et al. 455/461

FOREIGN PATENT DOCUMENTS

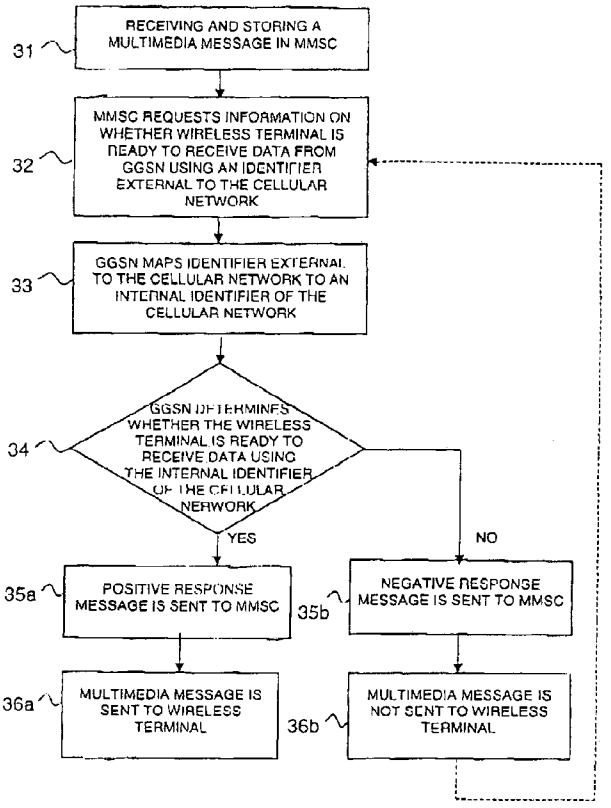
WO WO 99/61966 12/1999
WO WO 00/38438 6/2000

Primary Examiner—Temica M. Beamer
(74) *Attorney, Agent, or Firm*—Perman & Green, LLP

(57) **ABSTRACT**

A method is provided for inquiring about information relating to a mobile terminal of a cellular network, from a messaging server external to the cellular network. An inquiry is sent from the messaging server to the cellular network, comprising an external first identifier for identifying said terminal. In the cellular network the first identifier is mapped to a second internal identifier. The information relating to the terminal (MS) is determined with the aid of said second identifier and a responsive message is sent from the cellular network to said messaging server. In the response message, said information relating to the terminal is indicated by the first identifier.

19 Claims, 4 Drawing Sheets



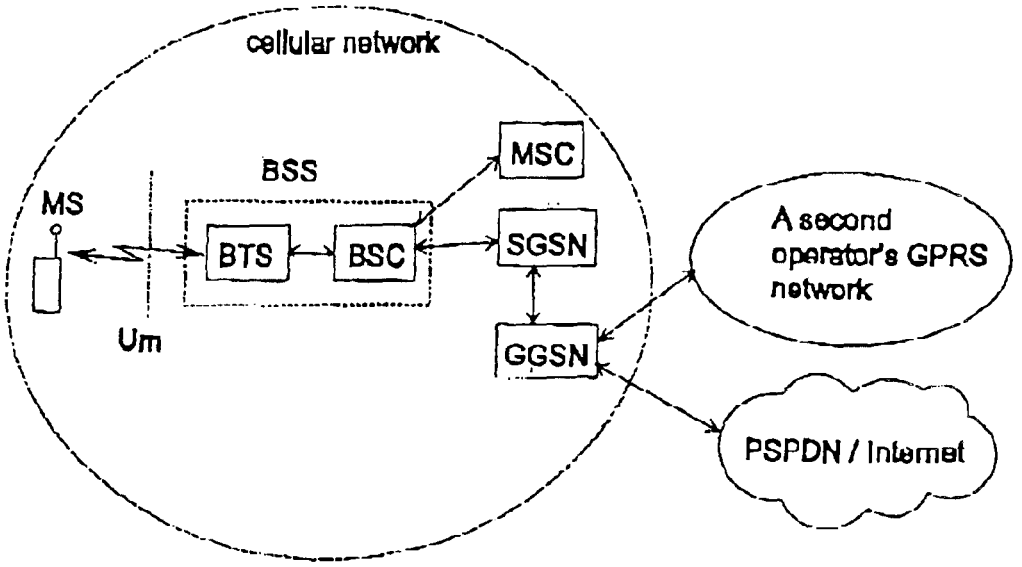


Fig. 1
PRIOR ART

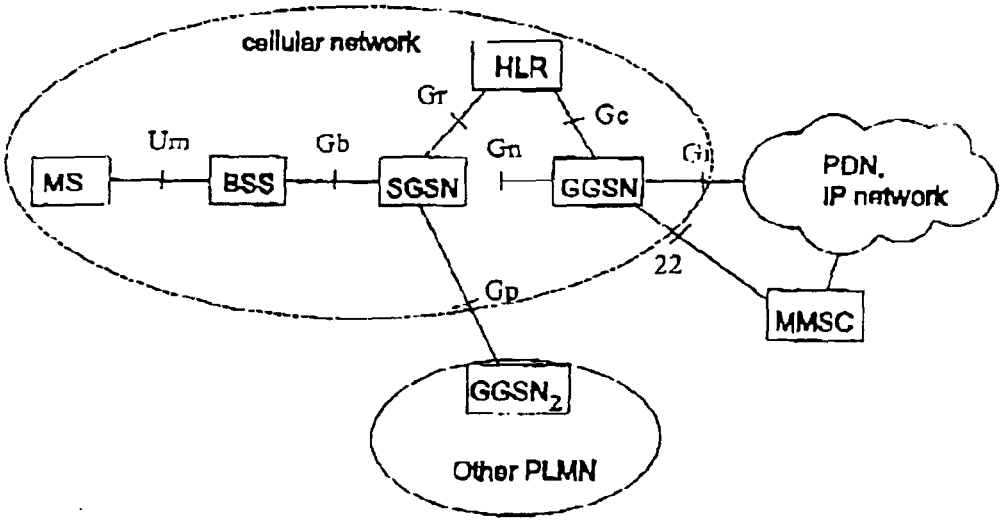


Fig. 2

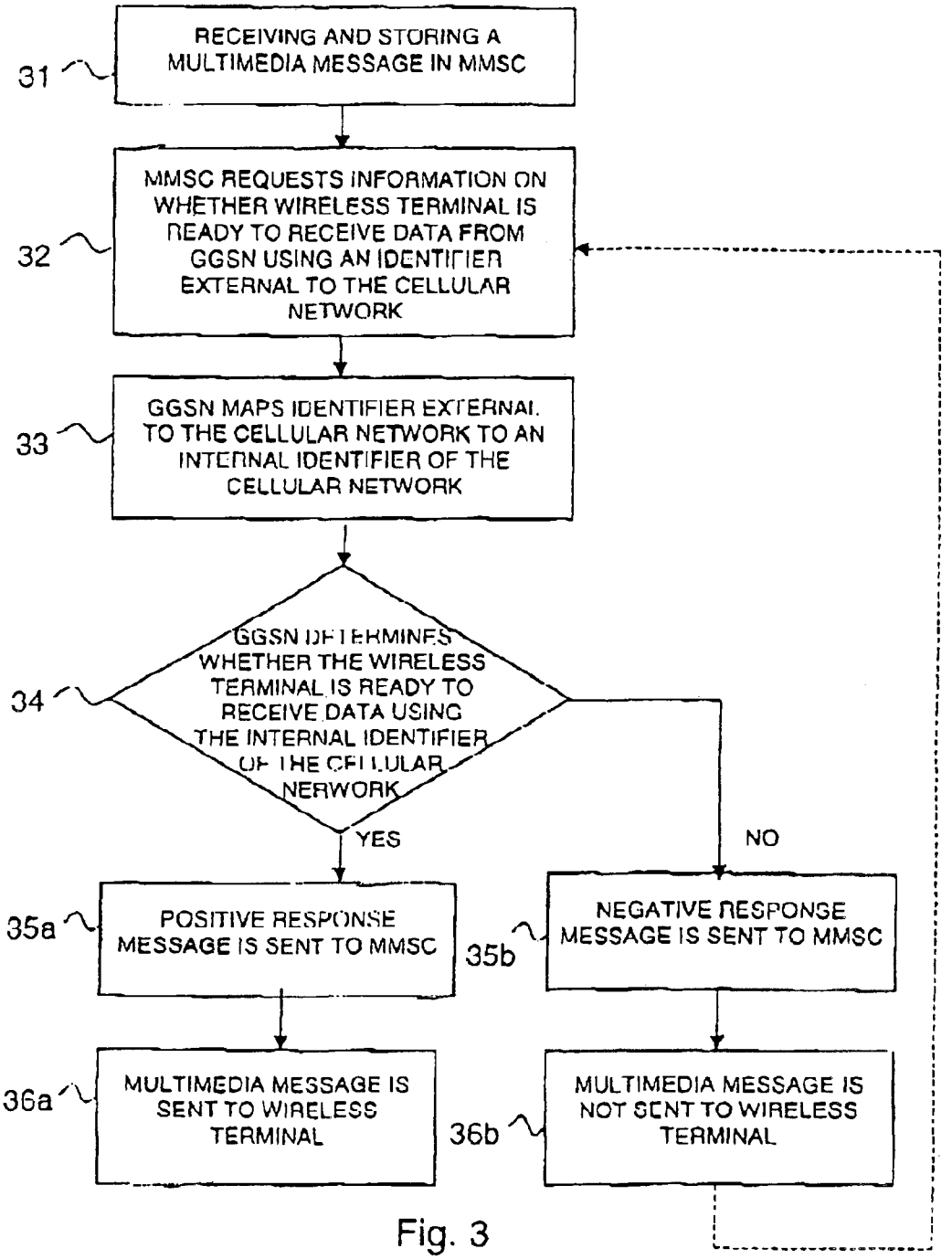

RECEIVING AND STORING A MULTIMEDIA MESSAGE IN MMSC
31
MMSC REQUESTS INFORMATION ON WHETHER WIRELESS TERMINAL IS READY TO RECEIVE DATA FROM GGSN USING AN IDENTIFIER EXTERNAL TO THE CELLULAR NETWORK
32
GGSN MAPS IDENTIFIER EXTERNAL TO THE CELLULAR NETWORK TO AN INTERNAL IDENTIFIER OF THE CELLULAR NETWORK
33
GGSN DETERMINES WHETHER THE WIRELESS TERMINAL IS READY TO RECEIVE DATA USING THE INTERNAL IDENTIFIER OF THE CELLULAR NERWORK
34
YES
NO
POSITIVE RESPONSE MESSAGE IS SENT TO MMSC
35a
NEGATIVE RESPONSE MESSAGE IS SENT TO MMSC
35b
MULTIMEDIA MESSAGE IS SENT TO WIRELESS TERMINAL
36a
MULTIMEDIA MESSAGE IS NOT SENT TO WIRELESS TERMINAL
36b

Fig. 3

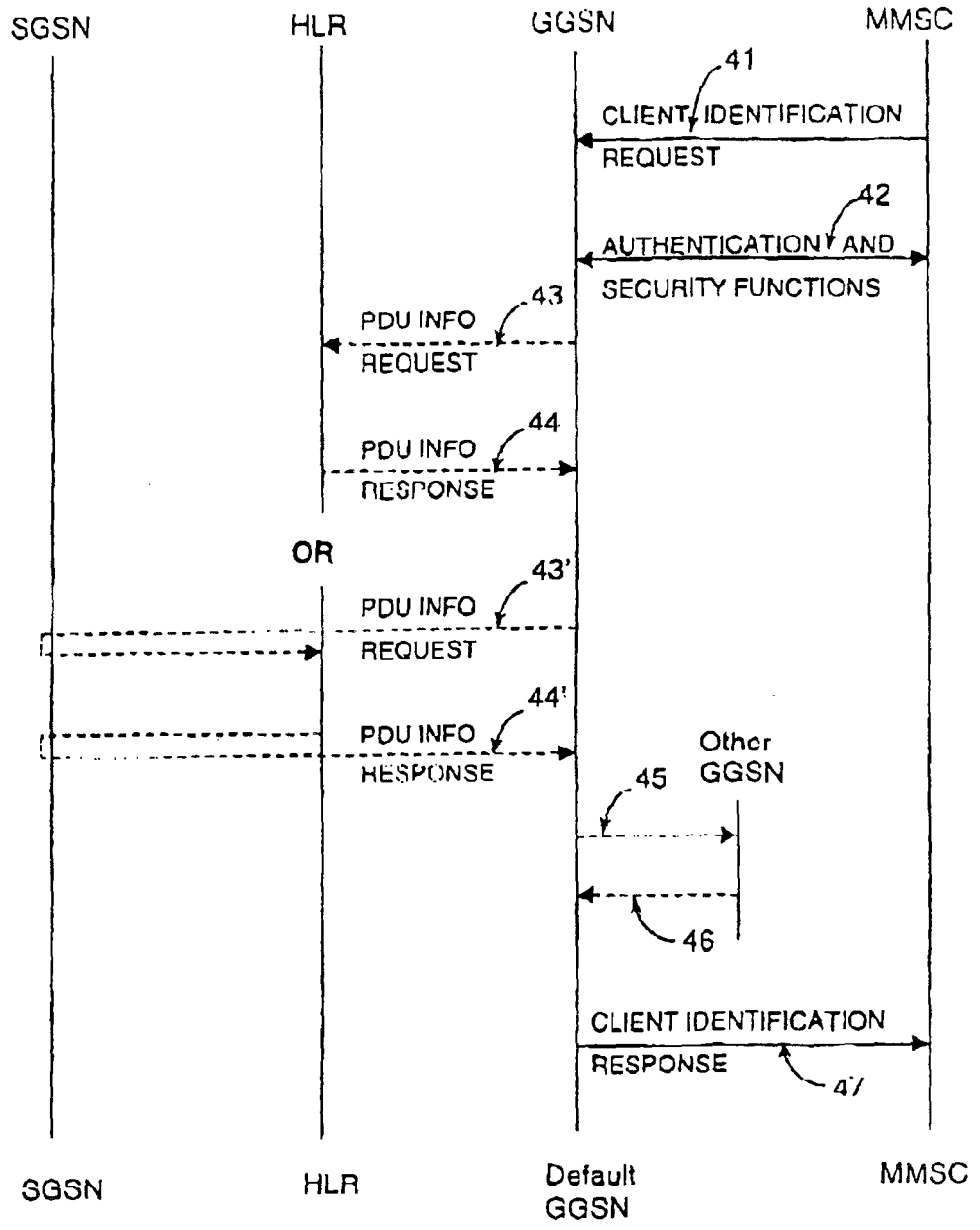

SGSN
HLR
GGSN
MMSC
41
CLIENT IDENTIFICATION
REQUEST
42
AUTHENTICATION AND
SECURITY FUNCTIONS
43
PDU INFO
REQUEST
44
PDU INFO
RESPONSE
OR
43'
PDU INFO
REQUEST
44'
PDU INFO
RESPONSE
Other
GGSN
45
46
CLIENT IDENTIFICATION
RESPONSE
47
SGSN
HLR
Default
GGSN
MMSC

Fig. 4

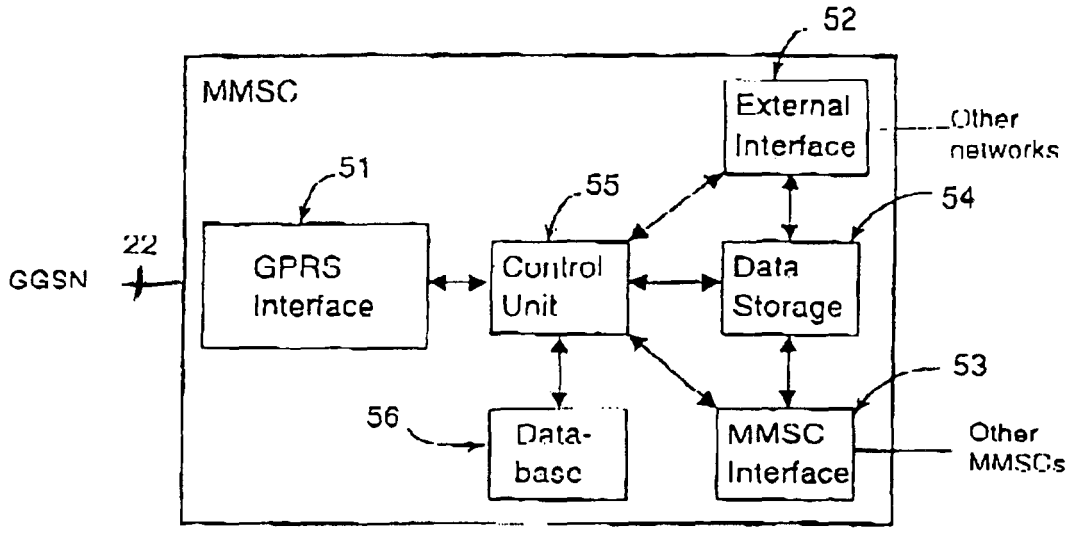

52
MMSC
External Interface
Other networks
51
55
54
22
GGSN
GPRS Interface
Control Unit
Data Storage
53
56
Data-base
MMSC Interface
Other MMSCs

Fig. 5

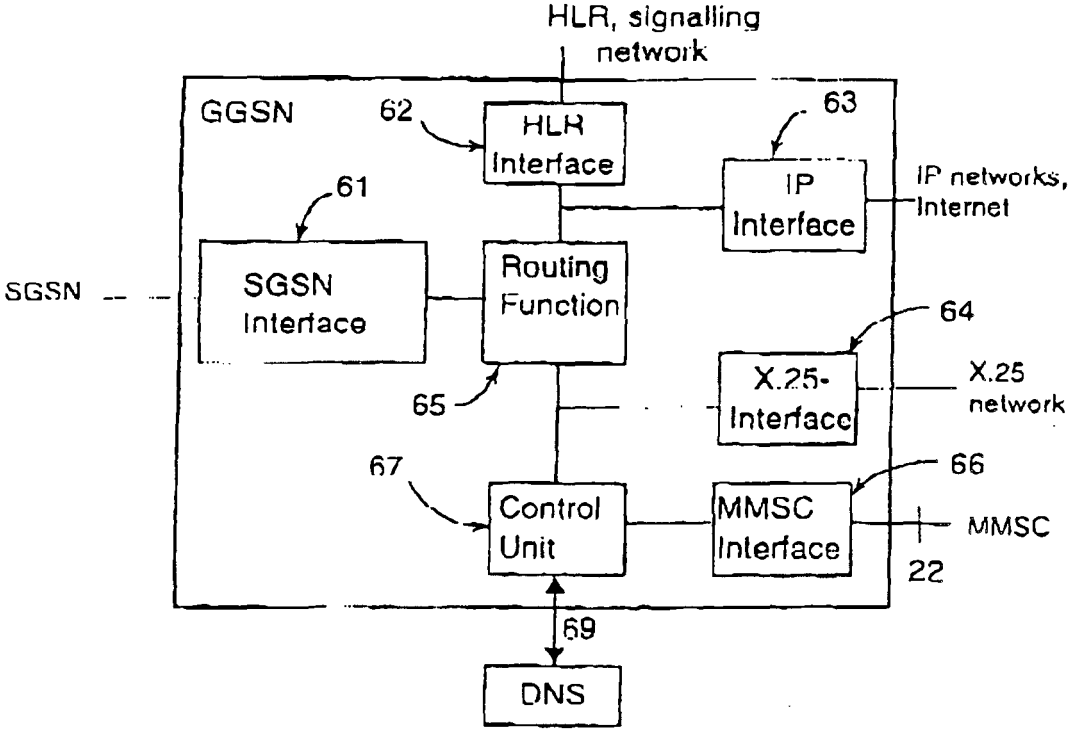

HLR, signalling network
GGSN
62
HLR Interface
63
IP Interface
IP networks, Internet
61
SGSN
SGSN Interface
Routing Function
64
X.25-Interface
X.25 network
65
67
66
Control Unit
MMSC Interface
MMSC
22
69
DNS

Fig. 6

TRANSFERRING OF A MESSAGE

FIELD OF THE INVENTION

The present invention relates to a messaging service. In particular, but not necessarily, the invention relates to the store-and-forward messaging of multimedia messages in a wireless telecommunication system.

BACKGROUND OF THE INVENTION

Wireless communication networks and the Internet network are expanding rapidly and their number of users is increasing. The GPRS (General Packet Radio Service) of the GSM (Global System for Mobile Communications) provides means for transferring information in packet switched mode in a cellular radio network. GPRS also provides an interface to other packet switched networks, such as the Internet network.

FIG. **1** shows the interconnections of a telecommunication network in a packet switched GPRS service. The main element of the network's infrastructure for providing GPRS services is a GPRS support node. GPRS support nodes are categorised into Serving GPRS Support Nodes SGSN which, in packet switched data transmission correspond to the Mobile Switching Centers MSC of the GSM network, known in connection with circuit switched data transmission, and Gateway GPRS Support Nodes GGSN. An SGSN is a support node that transmits data packets to a wireless terminal MS (Mobile Station) and receives data packets transmitted by a wireless terminal through a Base Station System BSS, comprising base transceiver stations BTS and base station controllers BSC. In this description, the term wireless terminal MS is used to mean all terminals that communicate over a specific radio interface. Thus, a computer terminal that communicates through a mobile station attached thereto will also be referred to as a wireless terminal. The SGSN also maintains information on the location of the wireless terminals that move in its service area in GPRS registers (not shown in FIG. **1**). Physically, the SGSN is typically implemented as a separate network element. The GGSN that communicates with the SGSN provides a connection to and enables co-operation with other networks. Such networks can be, among others, another operator's GPRS (cellular) network or a private network such as, for example, a company's Intranet network, a public switched packet data network PSPDN such as, for example, the Internet network or an X.25 network.

For a long time, the user of a computer terminal in communication with the Internet network has had the opportunity to retrieve multimedia components, such as pictures, text, short video clips and audio clips in electronic format, into his computer terminal from a server of the Internet network. As data transfer rates increase and the properties of mobile stations improve, an interest in a multimedia messaging service and messaging services in general has now also been awakened in wireless networks. As networks that support packet switched data transmission, the GPRS network and 3rd generation mobile communication networks, such as CDMA2000 (Code Division Multiple Access) and WCDMA (Wideband CDMA) in particular, are very well suited for the implementation of a multimedia messaging service.

A multimedia messaging service for 3rd generation mobile communication networks has been proposed which would be implemented in a manner similar to the Short Message Service SMS in a GSM network, i.e. substantially in a store-and-forward manner by transferring messages addressed to a wireless terminal, stored in a specific messaging server, to the wireless terminal when it can be contacted. Said messaging server would preferably be located outside the cellular network in question, for example, in the Internet network.

In the following, a GPRS network will be examined. In the GPRS service of the GSM network, a wireless terminal "attached" to the GPRS network can transmit and receive short messages. The wireless terminal can transmit and receive data in packet switched mode if it is attached to the GPRS network and, in addition, it has an active PDP-context (PDP=Packet Data Protocol) with some GGSN. Activation of a PDP-context may be effected either at the request of the wireless terminal or the network.

It is expedient for the messaging server to make specific inquiries to the GPRS network from time to time. For example, on receiving a message addressed to a given wireless terminal, it is expedient for the messaging server to make sure, by making an inquiry, that the wireless terminal in question is actually ready to receive the message (i.e. it has an active PDP-context with some GGSN), before transmitting the message to the GPRS network . In cellular networks, dynamic PDP addresses (such as dynamic IP addresses, Internet Protocol) are often allocated to terminals. In this case, a wireless terminal does not necessarily always have use of the same PDP address, but when a wireless terminal requests a PDP address, the network gives it a PDP address, which may be the same PDP address the wireless terminal had on a previous occassion, or some other PDP address, depending on what PDP addresses the network has free at that time for the use of wireless terminals.

When using dynamic IP addresses there is a problem associated with performing the previously mentioned inquiry to identify said wireless terminal from outside the cellular network (GPRS network): How can a wireless terminal be identified from outside a cellular network so that inquiries relating to the wireless terminal can also be carried out reliably when the wireless terminal has a dynamic PDP address?

SUMMARY OF THE INVENTION

Now, a new solution has been invented relating to the identification of a wireless terminal. According to a first aspect of the invention, there is provided a method for inquiring about information relating to a terminal of a cellular network from the cellular network, from a messaging server external to the cellular network.

The method is characterised in that it comprises:

sending an inquiry from the messaging server to the cellular network to determine said information relating to the wireless terminal, the inquiry comprising a first identifier for identifying said terminal, the first identifier being a specific identifier external to the cellular network;

mapping said first identifier to a specific second identifier in the cellular network, the second identifier being an internal identifier of the cellular network;

determining said information relating to the terminal with the aid of said second identifier;

sending a response message in response to said inquiry from the cellular network to said messaging server external to the cellular network, in which response message said information relating to the terminal is indicated with the aid of said first identifier.

According to a second aspect of the invention, there is provided a server external to a cellular network for inquiring

about specific information relating to a terminal of the cellular network from the cellular network

The server is characterised in that it server comprises:

means for defining a specific first identifier external to the cellular network for identifying said terminal;

means for sending an inquiry from the server to the cellular network to determine said information relating to the terminal, the inquiry comprising said first identifier.

According to a third aspect of the invention, there is provided a computer program product executable in a server external to a cellular network for inquiring about specific information relating to a terminal of the cellular network from the cellular network.

The computer program product is characterised in that it comprises program code:

for defining a specific first identifier external to the cellular network for identifying said terminal;

for causing said server to send an inquiry to the cellular network to determine said information relating to the terminal, the inquiry comprising said first identifier for identifying said terminal.

According to a fourth aspect of the invention, there is provided a network element of a cellular network.

The network element is characterise in that it comprises:

means for receiving a specific inquiry sent by a server external to the cellular network, the inquiry comprising a request to determine specific information relating to a terminal of the cellular network, and the inquiry comprising a first identifier for identifying said terminal, the first identifier being a specific identifier external the cellular network;

means for mapping said first identifier to a specific second identifier, the second identifier being an internal identifier of the cellular network;

means for determining said information relating to the terminal with the aid of said second identifier;

means for sending a response message to the server external to the cellular network in response to said inquiry, the response message comprising the information relating to said terminal indicated with the aid of said first identifier.

According to a fifth aspect of the invention, there is provided a computer program product executable in a network element of a cellular network.

The computer program product is characterised in that it comprises program code:

for causing the network element to receive a specific inquiry sent by a server external to the cellular network, the inquiry comprising a request to determine specific information relating to a terminal of the cellular network, and the inquiry comprising a first identifier for identifying said terminal, the first identifier being a specific identifier external to the cellular network;

for mapping said first identifier to a specific second identifier, the second identifier being an internal identifier of the cellular network;

for causing the network element to determine said information relating to the terminal with the aid of said second identifier;

for causing the network element to send a response message to the server external to the cellular network in response to said inquiry, the response message comprising the information relating to said terminal indicated with the aid of said first identifier.

According to a sixth aspect of the invention, there is provided a system, comprising a server external to a cellular network and a network element of the cellular network for inquiring about information relating to a terminal of the cellular network from the cellular network, from the server external to the cellular network.

The system is characterised in that the server comprises:

means for defining a specific first identifier external to the cellular network for identifying said terminal;

means for sending an inquiry from the server to the network element of the cellular network to determine said information relating to the terminal, the inquiry comprising said first identifier, and that the network element of the cellular network comprises:

means for receiving said inquiry;

means for mapping said first identifier to a specific second identifier, the second identifier being an internal identifier of the cellular network;

means for determining said information relating to the terminal with the aid of said second identifier;

means for sending a response message to the server external to the cellular network in response to said inquiry, the response message comprising the information relating to said terminal indicated with the aid of said first identifier.

In this description, the terminal can be any wireless terminal that can be attached to a GPRS network or a 3^{rd} generation network, for example, a mobile station of a cellular network or a computer terminal attached to a GPRS network (e.g. through a telephone of a cellular network). In connection with the present application, the concept of a cellular network should be interpreted broadly, whereupon the concept of a cellular network is also considered to cover, for example, the GPRS service of a GSM network and the network elements of the core network of a 3^{rd} generation network. In a preferred embodiment of the invention, said server is a messaging server, even more preferably a multimedia messaging server, located outside the cellular network in a packet data network, such as the Intranet network of an operator, the Internet network or an X.25 network.

In a preferred embodiment of the invention, said inquiry sent from the server to the cellular network to inquire about information relating to the terminal of the cellular network is addressed to a specific network element of a GPRS network, to a GGSN, which determines said information relating to the terminal of the cellular network, which can be, e.g. whether the terminal is attached to the GPRS network or whether the terminal is ready to receive data, and indicates it to said server external to the cellular network.

A specific first identifier external to the cellular network is used to identify the terminal between the server and the cellular network which, in connection with a preferred embodiment of the invention, is called an MMS-ID. Said first identifier is mapped to a specific second identifier in the cellular network. Said second identifier, which is an internal identifier of the cellular network and which can be, for example, the terminal's IMSI (International Mobile Subscriber Identity) code or an equivalent, is used to identify the terminal inside the cellular network and it is not revealed to network elements external to the cellular network.

BRIEF DESCRIPTION OF THE DRAWINGS

In the following, the invention will be described in detail with reference to the accompanying drawings, in which

FIG. **1** shows the interconnections of a telecommunication network in a packet switched GPRS service;

FIG. **2** illustrates an arrangement for implementing message transmission according to the invention;

FIG. **3** is a flow diagram illustrating a method for implementing a messaging service according to the invention; and

FIG. **4** is a message diagram showing the flow of messages in a method according to the invention;

FIG. **5** is a block diagram illustrating functional blocks of an MMSC; and

FIG. **6** is a block diagram illustrating functional blocks of a GGSN.

DETAILED DESCRIPTION

FIG. **1** was described above in connection with the description of prior art.

FIG. **2** illustrates an arrangement according to a first preferred embodiment of the invention for implementing message transmission between a wireless terminal MS that supports GPRS and a messaging server. FIG. **2** shows a wireless terminal MS, a Base Station System BSS, a Serving GPRS Support Node SGSN, and a Gateway GPRS Support Node GGSN, a Gateway GPRS Support Node $GGSN_2$ located in the mobile communication network PLMN (Public Land Mobile Network) of a second operator, a Packet Data Network PDN, which in a preferred embodiment of the invention is an IP network, a messaging server that is in communication with the IP network which, in a first preferred embodiment of the invention is a Multimedia Messaging Service Centre MMSC, and a Home Location Register HLR that contains the routing information and the GPRS subscription information of the wireless terminal MS. In this description, the term IP network means either an Intranet network managed by a company and/or an operator, or the open public Internet network.

FIG. **2** also shows the interfaces between different network elements: a Um interface between the wireless terminal MS and the base station system BSS, a Gb interface between the base station system BSS and the SGSN, a Gn interface between the SGSN and the GGSN, a Gi interface between the GGSN and the IP network, a Gr interface between the SGSN and the home location register HLR, a Gc interface between the GGSN and the home location register HLR, as well as a logical interface **22** according to the invention between the GGSN and the MMSC. In addition, FIG. **2** shows a logical Gp interface between the GPRS cellular networks of different operators.

Technically, the GPRS support nodes of a particular operator are connected to each other within the cellular network by the operator's internal IP network (Intra-PLMN Backbone). However, this should not be confused with the previously mentioned Intranet network, which is external to cellular network and is managed by a company and/or an operator However, said IP networks (the Intra-PLMN Backbone network and the Intranet network managed by the operator) are preferably functionally connected to each other, for example, through a gateway.

By agreement between operators, the GPRS networks of different operators are connected by a GPRS network (Inter-PLMN Backbone) between the operators. In practice, there is typically a firewall and a Border Gateway BG between the Intra-PLMN Backbone network and the Inter-PLMN Backbone network. These are not shown in FIG. **2**.

Among other things, the purpose of interface **22** is to enable messaging between the MMSC and the GGSN so that the GGSN can process an inquiry coming from the MMSC and respond to it. The MMSC is located outside the cellular network, preferably in the Intranet network of an operator. Preferably the interface **22** is implemented using the same protocol as that used in the operator's Intra-PLMN Backbone network, i.e. an IP protocol. Alternatively, the interface **22** can be implemented using some other protocol of the same level.

FIG. **3** is a flow diagram illustrating the general outline of a method for implementing a messaging service according to the first preferred embodiment of the invention. The method comprises determining the readiness of the wireless terminal MS to receive data, transferring information about this to an MMSC and, in the case where the wireless terminal MS is ready to receive data, transferring a multimedia message from the MMSC through the GPRS network to the wireless terminal MS.

First, a multimedia message addressed to the wireless terminal arrives at the MMSC and the MMSC stores it in its memory (block **31**). Next, the MMSC sends an inquiry to the GGSN through the interface **22**, i.e. a message-requesting information from the GGSN on whether the wireless terminal MS, to which the multimedia message is addressed, is ready to receive data (block **32**). According to the invention, a specific identifier MMS-ID external to the cellular network, to be presented later, is used in said inquiry to identify the wireless terminal. In block **33**, the GGSN maps said identifier external to the cellular network to a specific internal identifier of the cellular network (IMSI or equivalent). In block **34** the GGSN determines whether the wireless terminal MS is ready to receive data using said internal identifier of the cellular network. In the case of a GPRS network, the GGSN determines whether the wireless terminal has an active PDP-context with some GGSN. If the wireless terminal MS is ready to receive data (a PDP-context is activated with some GGSN), the GGSN sends a positive response message, again comprising said identifier external to the cellular network (block **35***a*), to the MMSC through the interface **22**, after which transfer of the multimedia message from the MMSC to the wireless terminal MS can start (block **36***a*). If the wireless terminal MS is not ready to receive data (a PDP-context is not activated), the GGSN sends a negative response message comprising said identifier external to the cellular network to the MMSC through the interface **22** (block **35***b*), whereupon transfer of the multimedia message from the MMSC to the wireless terminal MS cannot be started at that time (**36***b*). This being the case, the inquiry to determine the readiness of the wireless terminal MS to receive data can be repeated, for example, after a certain period of time (dashed line to block **32**).

Said multimedia message may comprise a plurality of multimedia elements, such as pictures, text, short video clips and audio clips in electronic format. The address of the recipient of the multimedia message associated with the multimedia message can be, for example, the telephone number of the wireless terminal MS, the logical network address of a computer terminal attached to the GPRS network or some other address supported by GPRS. Typically, said address is in RFC822 format. RFC822 is an Internet standard that defines a format in which a logical address can be presented in a form understandable to the user. An example of an address in RFC822 format is outi.aho@mmsc1.nokia1.com. Here, "mmsc1.nokia1.com" is the logical address (so-called domain name) of the MMSC in question. The telephone number of a is wireless terminal can also be converted into RFC822 format in an IP network. URL (Uniform Resource Locator) pointers can also be attached to said multimedia message.

Typically, the MMSC always sends the inquiry related to the readiness of said wireless terminal MS to receive data to the same GGSN, which will be called a "default-GGSN"

from now on. The address of the default-GGSN (typically indicated as a logical domain name which can be, e.g. in the form ggsn1.nokia1.com) is stored in the MMSC. The MMSC is located in a packet data network. Preferably, the MMSC is located outside the GPRS cellular network in the IP network (Intranet network) of the operator that also manages said default-GGSN. Alternatively, the MMSC can be managed by an external service provider, for example, in the Internet network.

The address of the recipient of the multimedia message in plain RFC822 format, stored in the MMSC, is mapped in the MMSC to a specific identifier, external to the cellular network, which is then used as an identifier for the wireless terminal MS in communication between the default-GGSN and the MMSC. In this description, said external identifier is called an MMS-ID (Multimedia Messaging Service Identity). To perform the mapping, the MMSC comprises a specific database, in which the wireless terminal's multimedia messaging service subscription information is stored. The correspondences between the MMS-ID and the the wireless terminal's addresses in RFC822 format are also stored in said database. Said database of the MMSC is presented in connection with the description of FIG. **5**.

The MMS-ID is an identifier external to the of the cellular network, a parameter or a set of parameters, which indicates the MMSC from which the wireless terminal MS in question (the owner of the terminal) has subscribed to a multimedia messaging service. The MMS-ID has a general data format, so it can be, for example, in a text format and, for example, may appear as follows:

|MMSC ID|User ID|Security ID|,

where a vertical line (|) separates the different parts of the MMS-ID, which are for example, an MMSC ID, which is the identifier of the MMSC in question, a User ID, which is the identifier of the (multimedia messaging) service subscriber, and a Security ID, which can be formed in the MMSC and the default-GGSN on the basis of the MMSC ID and the User ID using a specific algorithm agreed upon in advance. The Security ID can be used in the cellular network to ensure the legitimacy of the MMSC and the subscriber.

The correspondence between the MMS-ID and the IMSI code of the wireless terminal in question, which is an identifier internal to the cellular network, is stored in the GPRS network. The database in which it is stored, can be implemented in the GPRS network, for example, by means of a DNS (Domain Name System) server. The IMSI code is used as the principal identifier of the mobile subscriber of the wireless terminal MS within the GPRS network. Typically, the IMSI code is stored in a SIM (Subscriber Identity Module) card, The SIM card is used as a subscriber identity unit in the wireless terminal MS. Thus, when the present description refers to e.g. the IMSI code of a wireless terminal, this means the IMSI code of a subscriber known to the network, stored in a SIM card or the like, installed in the wireless terminal MS. Correspondingly, when a multimedia message addressed to the wireless terminal MS is mentioned, this means a multimedia message addressed to the subscriber whose SIM card is in the wireless terminal MS, and so on.

Depending on the implementation, the database in which the correspondences between the MMS-ID and the IMSI code of the wireless terminal are stored may be located in different places in the teleoperator's GPRS network. The database should be easy for the default-GGSN to access. Said database can also be implemented in an appropriate manner by means other than a DNS server. It is also possible to integrate said database into the HLR, but preferably this is not done, as there is a desire to keep the amount of data to be stored in the HLR as small as possible.

FIG. **4** shows a message diagram that illustrates the flow of messages between the MMSC and the parts of the GPRS network in a first preferred embodiment of the invention. Having mapped the address of the recipient into an MMS-ID, the MMSC sends an inquiry, in the form of a Client Identification Request message **41**, to the default-GGSN to determine the readiness of the wireless terminal to receive data. The MMS-ID is delivered with this message. After this, specific authentication and security functions **42** can be carried out to check that the MMSC in question is authorised to carry out said inquiry. Typically, the Security ID part of the MMS-ID is used here, in such a way that the default-GGSN forms a Security ID on the basis of the MMSC-ID and User ID comprised by the MMS-ID using a specific pre-determined algorithm and compares it to the Security ID (formed by the MMSC) delivered with the MMS-ID. Alternatively, some other security mechanism can be used.

The default-GGSN maps the MMS-ID delivered with the Client Identification Request message **41** to the IMSI code of the wireless terminal to which the MMS-ID in question belongs. The default-GGSN preforms said mapping by inquiring about the lMSI code that corresponds to said MMS-ID from the above-mentioned database, in which the correspondences between the MMS-ID and the IMSI code of the wireless terminal are stored (e.g. from the DNS server).

Next, the default-GGSN, which maintains the PDP-context parameters and fields (e.g. IP address) of wireless terminals, examines whether the wireless terminal having the IMSI code in question has an active PDP-context with the default-GGSN in question. If a PDP-context is active, the default-GGSN knows that the wireless terminal MS is ready to receive data. This being the case, the default-GGSN is also aware of the wireless terminal's IP address, regardless of whether it is statically or dynamically allocated. As a response to the inquiry, the default-GGSN now sends the MMSC a positive Client Identification Response message **47**, which indicates that the wireless terminal MS having the MMS-ID in question is ready to receive data. It is possible to indicate the IP address (either dynamic or static) of the wireless terminal that is ready to receive data in said positive Client Identification Response message **47**, or just to indicate that the wireless terminal MS having the MMS-ID in question is ready to receive data through the default-GGSN in question.

If the MMSC is logically connected with the GPRS (cellular) network, for example, in the operator's own Intranet network, interface **22** can subsequently be used for transmitting the multimedia message to the default-GGSN (and further to the wireless terminal MS). If the MMSC is located in a packet data network (e.g. in the Internet network) managed by an external service provider, typically, the multimedia message is also sent to the MS through the Internet network, According to the invention, the multimedia message is preferably no longer stored in any network element of the cellular network, but the data packets are delivered uninterrupted to the wireless terminal MS, This advantage is achieved by placing the MMSC outside the cellular network. Transmission of data from the packet data network to the GPRS network is well known to a person skilled in the art.

If the wireless terminal MS does not have an active PDP-context with the default-GGSN, the default-GGSN

determines whether the wireless terminal MS has an active PDP-context (an existing data connection) with some other GGSN Preferably, the default-GGSN finds this out by making an inquiry in the form of a PDU Info Request message **43** (PDU=Protocol Data Unit) over the Gc interface to the home location register HLR. Alternatively, if the Gc interface is not implemented in the system, the GGSN can send a PDU Info Request message **43'** over the Gn interface to the SGSN and request the SGSN to transfer the message **43'** over the Gr interface to the HLR.

Here it should be noted that the PDU Info Request message **43**, **43'** does not have to be transmitted at all if the wireless terminal MS has an active PDP-context with the default-GGSN, i.e. with the GGSN to which the Client Identification Request message **41** was originally sent from the MMSC. Therefore, the PDU Info Request message **43**, **43'** and the PDU Info Response message **44**, **44'** sent in due course as a response, are shown with dashed lines in FIG. **4**.

The HLR maintains the GPRS subscriber information of wireless terminals. Among other things, information on the PDP-contexts a wireless terminal having a specific IMSI code is permitted to activate is found in the HLR's "PDP context subscription records" fields. The "PDP context subscription records" fields also comprise an "Access Point Name" field (APN) that indicates, for each IMSI, the Access Points at which a particular wireless terminal MS is permitted to connect to an external packet data network. Here the term external packet data network means the Internet network, for example. On receiving the PDU Info Request message **43**, **43'**, in the next step of the method the HLR checks the logical names of the access points permitted to the IMSI in question from the APN field, on the basis of the IMSI code of the wireless terminal MS in question sent with the PDU Info Request message **43**, **43'**.

Said logical names of the access points are sent by the HLR to the default-GGSN in a PDU Info Response message **44**, **44'**. The PDU Info Response message is sent from the HLR to the default-GGSN, either directly through the Gc interface (message **44**) or via the SGSN over the Gr and Gn interfaces (message **44'**). The access point names indicate the GGSNs, with which the wireless terminal MS can have an active PDP-context, to the default-GGSN. A PDP-context can be activated, for example, with another GGSN of the same GPRS network or with a GGSN of a GPRS network (other PLMN) controlled by another teleoperator, such as $GGSN_2$ (FIG. **2**).

In the next step, the default-GGSN to which the original inquiry from the MMSC arrived, determines if any of the GGSNs with which, on the basis of the PDU Info Response message, the wireless terminal MS may have a PDP-context activated, actually has an active context. This investigation is made by sending said GGSNs a message **45** (Other GGSN, FIG. **4**), which forwards the IMSI code of the wireless terminal in question and requests each GGSN to examine its own PDP-context fields on the basis of said IMSI code to determine whether the wireless terminal in question has an active PDP-context with the GGSN in question. GGSNs controlled by the same operator are interconnected by the operator's internal IP network (Intra-PLMN Backbone network), whereupon the domain name of each GGSN can be used as the address of the recipient of the investigation message **45**. Investigation messages **45** can be sent to the GGSNs of another operator through the Gp interface between different operators, defined in GPRS, or over the Internet via the Gi interface. However, the Gi interface is preferably not used because, for security reasons, there is a desire not to reveal the secret IMSI code of the wireless terminal to network elements external to the GPRS network. Each GGSN to which said message is sent, responds **46** to the default-GGSN that sent the message **45**, indicating whether the GGSN in question has an active PDP-context with the wireless terminal MS having the IMSI code in question. In the case where a particular GGSN has an active PDP-context with the wireless terminal MS in question, the response message preferably comprises the PDP address (e.g. IP address) of the wireless terminal in question, particularly if it is of the dynamic type. Said information is apparent from the values of the wireless terminal's PDP-context parameters, maintained by the GGSN in question.

On receiving the responses **46**, the default-GGSN sends either a positive or negative Client Identification Response message **47** over interface **22** to the MMSC. A positive Client Identification Response message **47** comprises information that the wireless terminal having the MMS-ID in question is ready to receive data via a specific GGSN. Preferably, the message **47** contains the MMS-ID in question. Said specific GGSN is the GGSN with which the wireless terminal MS has an active PDP-context. If the wireless terminal has active PDP-contexts with more than one GGSN, the addresses of all these GGSNs can be communicated to the MMSC. It is also possible to indicate the PDP address, such as the IP address, of the wireless terminal ready to receive data in said positive Client Identification message **47**.

A negative Client Identification Response message **47** comprises information that the wireless terminal having the MMS-ID in question is not ready to receive data, whereupon the MMSC can, for example, send a new inquiry to the default-GGSN to determine the readiness of the wireless terminal MS to receive data, a specific period of time after sending the previous inquiry.

Alternatively, the default-GGSN can check the wireless terminal's readiness to receive data by sending a slightly modified PDU Info Request message **43**, **43'** to the HLR. In this case, the HLR first looks up the address of the SGSN serving the wireless terminal at that particular moment, from the SGSN Address field maintained in the HLR, and then inquires from the SGSN in question on the basis of the IMSI code of the wireless terminal, over the Gr interface, whether the wireless terminal MS in question has an active PDP-context with some GGSN. The GGSN with which the wireless terminal MS has activated a PDP-context is apparent, e.g. from the value of the "GGSN Address in use" parameter maintained by the SGSN in question. On receiving the information it requested from the SGSN, the HLR further sends a PDU Info Response message **44**, **44'** to the default-GGSN, as described above. It is also possible that the HLR delivers the address of the SGSN serving the wireless terminal MS to the default-GGSN, after which the default-GGSN inquires about the address of the GGSN with which the wireless terminal MS has an active PDP-context from said SGSN, on the basis of the IMSI code.

According to the invention, a GGSN may also refuse to transfer a message from the MMSC to the wireless terminal. For example, if the wireless terminal's telephone bills have not been paid, the default-GGSN may return a negative Client Identification Response message **47** to the MMSC, in which it is-indicated that multimedia messaging to the wireless terminal MS in question is not permitted. Naturally, in this case, the database which maintains the wireless terminal's invoicing data in the GPRS network must be accessible to the default-GGSN. Typically, said negative Client Identification Response message **47** is also sent in a

situation, where the above-mentioned authentication and security functions **42** do not succeed. In this case, execution of the method according to the invention will also be halted in the cellular network before the MMS-ID is mapped to the IMSI.

After receiving a positive Client Identification Response message **47**, the MMSC sends the multimedia message as data packets to the GGSN with which the wireless terminal has an active PDP-context. Said GGSN forwards the data packets to the wireless terminal MS.

The MMSC can send the data packets to said GGSN via the default-GGSN or through a packet data network, such as an IP network (e.g. Intranet, Internet). If said GGSN is served by an MMSC different from that which communicated with the default-GGSN, the data packets can alternatively be sent to said GGSN through this second MMSC. IP protocols or other protocols supported by the GPRS network can be used for communication between the MMSC and the wireless terminal MS.

The multimedia message described in connection with the first preferred embodiment of the invention, which the MMSC transfers to the wireless terminal that has subscribed to the multimedia service, may originate from many different sources. It can be, for example, a photograph, fax, home-video clip or voice message sent in electronic format from one wireless terminal to another. It may also contain, for example, an electronic mail message sent from a TCP/IP network to the MMSC, comprising a multimedia component to be transferred to the wireless terminal, or any message comprising multimedia components. Although this description has mainly discussed multimedia messages, the invention is not restricted to a multimedia messaging service, but can be used in any similar messaging service.

Alternatively, a messaging service can be implemented in a pull-type mode. In this case, the messaging server sends the wireless terminal MS a notification message to indicate that a message addressed to the wireless terminal has been stored in its memory. After this, the wireless terminal can decide about retrieving said message from the messaging server to the wireless terminal MS. Said notification message can be transmitted to the wireless terminal MS as a short message (SMS), if it is attached to the GPRS network even if it does not have an active PDP-context activated with any GGSN. If the wireless terminal MS is, however, attached to the GPRS network (MS is in a GPRS attach mode), it is possible for said notification message, for example, to request the wireless terminal MS to activate a PDP-context to enable it to receive messages (e.g. multimedia messages from a messaging server).

According to a second preferred embodiment of the invention, an inquiry is made from the messaging server to determine whether the wireless terminal is attached to the GPRS network (GPRS attach) in order to know whether the wireless terminal can receive said notification message in the form of a short message. This is done after storing the message addressed to the wireless terminal by sending a slightly modified Client Identification Request message **41** from the MMSC to the default GGSN in which the default-GGSN is requested to determine whether the wireless terminal having the MMS-ID in question is attached to the GPRS network.

The default-GGSN maps the MMS-ID to the IMSI of the wireless terminal in question with the aid of the DNS server and checks whether the wireless terminal is attached to the GPRS network by sending a PDU Info Request message **43**, **43'** to the HLR. In this case, the HLR checks the SGSN Address field it maintains, according to the IMSI in question, to determine whether the SGSN Address field contains the SGSN address. If the SGSN address is found in the field in question said wireless terminal is attached to the GPRS network. If the SGSN Address field is empty said wireless terminal is not attached to the GPRS network.

Having determined whether said wireless terminal MS is attached to the GPRS network, the HLR sends a PDU Info Response message **44**, **44'** to the default-GGSN, which sends either a positive or negative Client Identification Response message **47** to the MMSC. The positive Client Identification Response message **47** indicates that the wireless terminal having the MMS-ID in question is attached to the GPRS network and is, therefore, ready to receive the notification messages as a short message. The negative Client Identification Response message **47** indicates that said wireless terminal MS is not attached to the GPRS network, in which case it is not yet appropriate to send the notification message.

In addition to a GPRS network, the invention can also be implemented in 3^{rd} generation networks, such as in a WCDMA network, because the uppermost protocol levels of such a network correspond to the uppermost protocol levels of a GPRS network. In a 3^{rd} generation network, a 3G-GGSN (3^{rd} Generation GGSN) corresponds to the GGSN, a 3G-SGSN corresponds to the SGSN and a 3G-RAN (3^{rd} Generation Radio Access Network) corresponds to the base station system BSS. According to one proposal, in a 3^{rd} generation network, an IMUI (International Mobile User Identity) code corresponds terminologically to the IMSI code, and a UIM (User Identification Module) card corresponds to the SIM card.

The invention is also suitable for implementation in a WAP system. In this case, a WAP gateway is situated between the MMSC and the default-GGSN, through which messages travelling between the MMSC and the default-GGSN typically pass transparently.

The invention can be implemented in software by making the required changes to the program code in the GGSN. The functionality of the MMSC can also be implemented programmably. The computer program products in question can be stored in a data medium, for example, in a memory, they can be transferred and they can be executed, for example, in a computer.

FIG. **5** shows a block diagram illustrating the functional blocks of an MMSC associated with implementation of the present invention. The MMSC comprises a GPRS interface **51** through which the MMSC communicates with a GGSN of a GPRS network. Communication with other external networks, such as the Internet, is managed through an external interface **52** and communication with other multimedia messaging service centres is handled through an MMSC interface **53**. Data store **54** is a database in which multimedia messages are stored and kept. A control unit **55** controls the operation of the MMSC. For mapping the plain (RFC822 address) of the recipient of a multimedia message to the correct MMS-ID, the MMSC comprises a database **56**, in which the correspondences between the plain addresses in RFC822 format and the MMS-IDs are maintained. Additionally, the MMSC comprises some blocks related to authentication and maintenance of the MMSC (these are not shown in the figure).

According to the invention, multimedia messages addressed to a wireless terminal MS arrive at the MMSC via one of its interfaces (**51–53**) and are stored in the data store **54**. On the basis of the data in database **56**, the control unit maps the plain address of the wireless terminal MS (e.g. an address in RFC822 format) into an MMS-ID. The database

56 can be maintained, for example, by a telecommunication network operator or a service provider external to the cellular network. A new MMS-ID can be added to said database 56, for example, as follows: When the owner of a specific wireless terminal MS subscribes to a multimedia messaging service, he/she tells the service provider the addresses of the wireless terminal MS he/she uses (e.g. telephone number, electronic mail-type address). The multimedia messaging service provider then agrees a suitable value for the MMS-ID by which the wireless terminal will be unequivocally identified with the GPRS operator question. Said addresses of the wireless terminal and the corresponding MMS-ID are stored in the database 56 of the MMSC. Correspondingly, the same MMS-ID is stored in a DNS server in the GPRS network under the control of the operator and is associated with the IMSI code that corresponds to the addresses in question. The inquiries (Client Identification Request) sent to the GGSN are preferably generated at the GPRS interface 51 at the command of the control unit 55, and its transmission takes place via the GPRS interface 51. The GPRS interface 51 and the MMSC interface 66 of the GGSN, presented in connection with the description of FIG. 6, together implement the interface 22. The response to the inquiry (Client Identification Response) sent by the GGSN is also received through the GPRS interface 51. The interface (51–53) of the MMSC through which multimedia messages are subsequently transmitted in to the wireless terminal MS may vary depending on the location of the MMSC and the wireless terminal.

FIG. 6 shows a block diagram illustrating the functional blocks of a GGSN associated with implementation of the present invention. The GGSN comprises an SGSN interface 61 through which the GGSN communicates with the cellular network managed by its own operator (Intra-PLMN Backbone network). The GGSN communicates with an HLR through an HLR interface 62. It is also possible to communicate with other elements of a signalling network (e.g. SS7) through this interface. The GGSN communicates with IP networks (e.g. the Internet) through an IP interface 63 and with an X-25 packet network through an X.25 interface 64, The GGSN transmits messages to the GPRS interface 51 of the MMSC and receives messages from the GPRS interface 51 of the MMSC, in a manner according to the invention, through an MMSC interface 66. The MMSC interface 66 and the GPRS interface 51 of the MMSC together implement the interface 22.

A routing function 65 routes data packets within the network managed by the operator and between the network managed by the operator and other networks. The DNS server is a separate device, typically controlled by the same operator as the GGSN. The GGSN control unit 67, which controls the operation of the GGSN, has a connection 69 to the DNS server. The DNS server contains information on the correspondence of the MMS-IDs and the IMSI codes of wireless terminals. Typically, the control unit 67 maps an MMS-ID arriving from the MMSC with a Client Identification Request message 41 to the correct IMSI code, in a manner according to the invention, by inquiring about the IMSI code the corresponds to said MMS-ID from the DNS server over said connection 69.

According to the present invention, an identifier external to a cellular network is used to identify a wireless terminal MS, such as an MMS-ID, which identifies the wireless terminal MS in question unequivocally, independent of the wireless terminal's address in RFC822 format used at any given time. Thus, the IMSI code used to unequivocally identify the wireless terminal inside the cellular network does not have to be revealed to outside the cellular network, Furthermore, use of an MMS-ID provides the advantage that if the address of the wireless terminal in RFC822 format changes, no changes are required in the cellular network (GPRS network). It is sufficient to update a new RFC822 address in the messaging server to correspond to the MMS-ID of the wireless terminal, which can still be used in communication between the messaging server and the cellular network.

The invention also enables inquiries relating to a wireless terminal to be performed from outside a cellular network in connection with the use of dynamic PDP addresses, because an MMS-ID independent of the dynamic PDP address is used in communication between the messaging server and the cellular network. Said inquiries are, for example, an inquiry to determine the readiness of a wireless terminal to receive data and an inquiry to determine whether a wireless terminal is attached to a GPRS network (i.e. an inquiry determine the readiness to receive a short message).

This description presents the implementation and embodiments of the present invention, with the aid of examples. It will be apparent to a person skilled in the art that the present invention is not restricted to details of the embodiments presented above, and that the invention can also be implemented in another form without deviating from the characteristics of the invention. The embodiments presented above should be considered illustrative, but not restrictive. Thus, the possibilities for implementing and using the invention are only restricted by the accompanying claims. Consequently, the various options for implementing the invention as determined by the claims, including equivalent implementations, also belong to the scope of the invention.

What is claimed is:

1. A method for inquiring about information relating to a wireless terminal of a cellular network, from the cellular network by a messaging server external to the cellular network, wherein the method comprises:

sending an inquiry from the messaging server to the cellular network to determine said information relating to the terminal, the inquiry comprising a first identifying said terminal, the first identifier being a specific identifier external to the cellular network;

mapping said first identifier to a specific second identifier in the cellular network, the second identifier being an internal identifier of the cellular network;

determining said information relating to the terminal with the aid of said second identifier;

sending a response message in response to said inquiry from the cellular network to said messaging server external to the cellular network, in which response message the information relating to said terminal is indicated with the aid of said first identifier.

2. A method according to claim 1, wherein said inquiry is made in response to a message addressed to the terminal arriving at the messaging server.

3. A method according to claim 2, wherein said message is a multimedia message.

4. A method according to claim 1, wherein the transmission of data in the method is performed in a packet switched mode.

5. A method according to claim 2, wherein the method comprises:

mapping an address associated with the message addressed to the terminal to said first identifier of the terminal in the messaging server before sending said inquiry to the cellular network.

6. A method according to claim 1, wherein said second identifier is one of the following: an IMSI (International Mobile Subscriber Identity) code, and IMUI (International Mobile User Identity) code.

7. A method according to claim 1, wherein said inquiry is sent to a specific network element of the cellular network and that said network element determines said information relating to the terminal (MS) using said second identifier.

8. A method according to claim 7, wherein said network element is a gateway GPRS support node and that the inquiry is always sent from the messaging server to the same gateway GPRS support node.

9. A method according to claim 2, wherein said network element is a gateway GPRS support node, and

said messaging server receives said response message, in which said information relating to the terminal is indicated, and that

said information is one of the following: the readiness of the terminal to receive data, the terminal being attached to the network.

10. A method according to claim 9, wherein said information relating to the terminal is the readiness of the terminal to receive data, whereupon said response message indicates whether said terminal has an active PDP-context (Packet Data Protocol) with a gateway GPRS support node, wherein:

in a situation, where the terminal has an active PDP-context with a gateway GPRS support node, said message is sent from the messaging server to the terminal in response to the receipt of said response message; and

in a situation, where the terminal does not have an active PDP-context with any gateway GPRS support node said message is not sent to the terminal.

11. A method according to claim 10, wherein in a situation, where the terminal does not have an active PDP-context with any gateway GPRS support node, said inquiry is repeated after a specific period of time.

12. A method according to claim 1, wherein said first identifier comprises:

a first part that indicates a messaging service subscriber;

a second part that indicates the messaging server in question; and

a third part that can be determined on the basis of said first and second parts for the purpose of security.

13. A server external to a cellular network for inquiring about specific information, relating to a terminal of the cellular network, from the cellular network, wherein the server comprises:

means for defining a specific first identifier external to the cellular network for identifying said terminal;

means for sending an inquiry from the server to the cellular network, the inquiry comprising said first identifier to be mapped in the cellular network to a specific second identifier so as to determine said information relating to the terminal with the aid of said second identifier, and wherein said second identifier is an internal identifier of the cellular network; and

means for receiving a response message sent from the cellular network in response to said inquiry, the response message comprising said determined information relating to said terminal, indicated with the aid of said first identifier.

14. A server according to claim 13, wherein the server is arranged to send said inquiry in response to a message addressed to the terminal arriving at the server; and that the server comprises:

means for mapping the address, associated with the message addressed to the terminal, to said first identifier of the terminal.

15. A computer program product executable in a server external to a cellular network for inquiring about specific information, relating to a terminal of the cellular network, from the cellular network, wherein the computer program product comprises:

program code for defining a first identifier external to the cellular network for identifying said terminal;

program code for causing said server to send an inquiry to the cellular network, the inquiry comprising said first identifier to be mapped in the cellular network to a specific second identifier so as to determine said information relating to the terminal with the aid of said second identifier, and wherein said second identifier is an internal identifier of the cellular network; and

program code for causing said server to receive a response message sent from the cellular network in response to said inquiry, the response message comprising said determined information relating to said terminal, indicated with the aid of said first identifier.

16. A network element of a cellular network, wherein it comprises;

means for receiving an inquiry sent by a server external to the cellular network, the inquiry comprising a request to determine specific information relating to a terminal of the cellular network, and the inquiry comprising a first identifier for identifying said terminal, the first identifier being a specific identifier external to the cellular network;

means for mapping said first identifier to a specific second identifier, the second identifier being an internal identifier of the cellular network;

means for determining said information relating to the terminal with the aid of said second identifier;

means for sending a response message to the server external to the cellular network in response to said inquiry, the response message comprising the information relating to said terminal indicated with the aid of said first identifier.

17. A network element according to claim 16, wherein said network element is a gateway support node of the cellular network.

18. A computer program executable in a network element of a cellular network, wherein the computer program product comprises program code:

for causing the network element to receive an inquiry sent by a specific server external to the cellular network, the inquiry comprising a request to determine specific information relating to a terminal of the cellular network, and the inquiry comprising a first identifier for identifying said terminal, the first identifier being a specific identifier external to the cellular network;

for mapping said first identifier to a specific second identifier, the second identifier being an internal identifier of the cellular network;

for causing the network element to determine said information relating to the terminal with the aid of said second identifier;

for causing the network element to send a response message to the server external to the cellular network in response to said inquiry, the response message comprising the information relating to said terminal indicated with the aid of said first identifier.

19. A system comprising a server external to a cellular network and a network element of the cellular network for inquiring about information, relating to a terminal of the cellular network from the cellular network from the server external to the cellular network, wherein the server comprises:

means for defining a specific first identifier external to the cellular network for identifying said terminal;

means for sending an inquiry from the server to the network element of the cellular network to determine said information relating to the terminal, the inquiry comprising said first identifier and that the network element of the cellular network comprises:

means for receiving said inquiry;

means for mapping said first identifier to a specific second identifier, the second identifier being an internal identifier of the cellular network;

means for determining said information relating to the terminal with the aid of said second identifier;

means for sending a response to the server external to the cellular network in response to said inquiry, the response message comprising the information relating to said terminal indicated with the aid of said first identifier.

* * * * *

US006885870C1

(12) EX PARTE REEXAMINATION CERTIFICATE (8597th)

United States Patent

Aho

(10) Number: US 6,885,870 C1

(45) Certificate Issued: Oct. 4, 2011

(54) **TRANSFERRING OF A MESSAGE**

(75) Inventor: **Outi Aho**, Lempäälä (FI)

(73) Assignee: **Comcast Cable Communications, LLC**, Philadelphia, PA (US)

Reexamination Request:
No. 90/011,318, Dec. 14, 2010

Reexamination Certificate for:
Patent No.: **6,885,870**
Issued: **Apr. 26, 2005**
Appl. No.: **09/745,756**
Filed: **Feb. 22, 2001**

(51) **Int. Cl.**
H04Q 7/22 (2006.01)

(52) **U.S. Cl.** **455/466**; 455/432.1; 455/432.3; 370/353; 370/395.1

(58) **Field of Classification Search** ..... None
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

6,717,928	B1	4/2004	Kalliokulju
6,728,208	B1	4/2004	Puuskari
7,127,489	B2	10/2006	Aho

FOREIGN PATENT DOCUMENTS

KR	19990060754 A	7/1999
WO	98/19438	5/1998
WO	99/66746	12/1999
WO	00/56088	9/2000
WO	00/64203	10/2000

OTHER PUBLICATIONS

Sevanto, Jarkko, "Multimedia Messaging Service for GPRS and UMTS," IEEE Wireless Communications and Networking Conference, IEEE WCNC 1999, pp. 1422–1426.

Wireless Application Protocol Push Architectural Overview, version Nov. 8, 1999, Wireless Application Protocol Forum, Ltd. (Nov. 8, 1999).

Wireless Application Protocol Push Proxy Gateway Service Specification, version Aug. 16, 1999, Wireless Application Protocol Forum, Ltd. (Aug. 16, 1999).

Wireless Application Protocol Push Access Protocol Specification, version Nov. 8, 1999, Wireless Application Protocol Forum, Ltd. (Nov. 8, 1999).

Wireless Application Protocol Push Message Specification, version Aug. 16, 1999, Wireless Application Protocol Forum, Ltd. (Aug. 16, 1999).

Wireless Application Protocol Push OTA Protocol Specification, version Nov. 8, 1999, Wireless Application Protocol Forum, Ltd. (Nov. 8, 1999).

Wireless Application Group User Agent Profile Specification, version Nov. 10, 1999, Wireless Application Protocol Forum, Ltd. (Nov. 10, 1999).

Wireless Application Protocol Wireless Application Environment Overview, version Nov. 4, 1999, Wireless Application Protocol Forum, Ltd. (Nov. 4, 1999).

Wireless Application Protocol Wireless Application Environment Specification Version 1.2, version Nov. 4, 1999, Wireless Application Protocol Forum, Ltd. (Nov. 4, 1999).

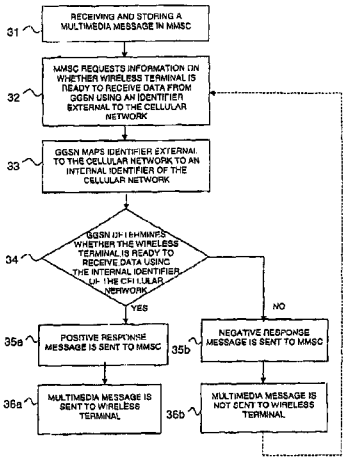
Wireless Application Protocol Architecture Specification, version Apr. 30, 1998, Wireless Application Protocol Forum, Ltd. (Apr. 30, 1998).

(Continued)

Primary Examiner—Roland Foster

(57) **ABSTRACT**

A method is provided for inquiring about information relating to a mobile terminal of a cellular network, from a messaging server external to the cellular network. An inquiry is sent from the messaging server to the cellular network, comprising an external first identifier for identifying said terminal. In the cellular network the first identifier is mapped to a second internal identifier. The information relating to the terminal (MS) is determined with the aid of said second identifier and a responsive message is sent from the cellular network to said messaging server. In the response message, said information relating to the terminal is indicated by the first identifier.



OTHER PUBLICATIONS

Wireless Application Protocol WAP over GSM USSD Specification, version Jul. 15, 1999, Wireless Application Protocol Forum, Ltd. (Jul. 15, 1999).
Wireless Application Protocol Binary XML Content Format Specification Version 1.2, version Nov. 4, 1999, Wireless Application Protocol Forum, Ltd. (Nov. 4, 1999).
Wireless Application Protocol Wireless Control Message Protocol Specification, version Aug. 4, 1999, Wireless Application Protocol Forum, Ltd. (Aug. 4, 1999).
Wireless Application Protocol Wireless Datagram Protocol Specification, version Nov. 5, 1999, Wireless Application Protocol Forum, Ltd. (Nov. 5, 1999).
Wireless Application Protocol WDP and WCMP Adaptation for access of a WAP Proxy Server to a Wireless Data Gateway, Wireless Application Protocol Forum, Ltd. (Nov. 5, 1999).
Wireless Application Protocol Identity Module Specification Part: Security, version Nov. 5, 1999, Wireless Application Protocol Forum, Ltd. (Nov. 5, 1999).
Wireless Application Protocol Wireless Markup Language Specification Version 1.2, version Nov. 4, 1999, Wireless Application Protocol Forum, Ltd. (Nov. 4, 1999).
Wireless Application Protocol WMLScript Language Specification Version 1.1, approved version Nov. 4, 1999, Wireless Application Protocol Forum, Ltd. (Nov. 4, 1999).
Wireless Application Protocol WMLScript Statement of Intent, version Apr. 30, 1998, Wireless Application Protocol Forum, Ltd. (Apr. 30, 1998).
Wireless Application Protocol WMLScript Standard Libraries Specification Version 1.1, approved version Nov. 4, 1999, Wireless Application Protocol Forum, Ltd. (Nov. 4, 1999).
Wireless Application Protocol Wireless Session Protocol Specification, version Nov. 5, 1999, Wireless Application Protocol Forum, Ltd. (Nov. 5, 1999).
Wireless Application Protocol Wireless Transport Layer Security Specification, version Nov. 5, 1999, Wireless Application Protocol Forum, Ltd. (Nov. 5, 1999).
Wireless Application Protocol Wireless Transaction Protocol Specification, version Jun. 11, 1999, Wireless Application Protocol Forum, Ltd. (Jun. 11, 1999).

EX PARTE REEXAMINATION CERTIFICATE ISSUED UNDER 35 U.S.C. 307

THE PATENT IS HEREBY AMENDED AS INDICATED BELOW.

Matter enclosed in heavy brackets [ ] appeared in the patent, but has been deleted and is no longer a part of the patent; matter printed in italics indicates additions made to the patent.

AS A RESULT OF REEXAMINATION, IT HAS BEEN DETERMINED THAT:

The patentability of claims **13-15** and **18-19** is confirmed.

Claims **1** and **16** are determined to be patentable as amended.

Claims **2-12** and **17**, dependent on an amended claim, are determined to be patentable.

New claims **20-113** are added and determined to be patentable.

1. A method for inquiring about information relating to a wireless terminal of a cellular network, from the cellular network by a messaging server external to the cellular network, wherein the method comprises:

sending an inquiry from the messaging server to the cellular network to determine said information relating to the terminal, the inquiry comprising a first *identifier* identifying said terminal, the first identifier being a specific identifier external to the cellular network;

mapping said first identifier to a specific second identifier in the cellular network, the second identifier being an internal identifier of the cellular network;

determining said information relating to the terminal with the aid of said second identifier;

sending a response message in response to said inquiry from the cellular network to said messaging server external to the cellular network, in which response message the information relating to said terminal is indicated with the aid of said first identifier.

16. A network element of a cellular network, wherein it comprises**[:]**:

means for receiving an inquiry sent by a server external to the cellular network, the inquiry comprising a request to determine specific information relating to a terminal of the cellular network, and the inquiry comprising a first identifier for identifying said terminal, the first identifier being a specific identifier external to the cellular network;

means for mapping said first identifier to a specific second identifier, the second identifier being an internal identifier of the cellular network;

means for determining said information relating to the terminal with the aid of said second identifier;

means for sending a response message to the server external to the cellular network in response to said inquiry, the response message comprising the information relating to said terminal indicated with the aid of the said first identifier.

20. A server according to claim 13, wherein the server is configured to send the inquiry to a gateway element of the cellular network.

21. A server according to claim 20, wherein the gateway element is a 3G-GGSN.

22. A server according to claim 13, wherein the server is configured to send the inquiry to, and to receive the response message from, the same element of the cellular network.

23. A server according to claim 13, wherein the information relating to the terminal comprises the readiness of the terminal to receive data.

24. A server according to claim 13, wherein the server is configured to repeat the inquiry as a result of a response message indicating the terminal is not ready to receive data.

25. A server according to claim 13, wherein said first identifier comprises:

a first part that indicates a messaging service subscriber; and

a second part that indicates the server.

26. A server according to claim 13, wherein the information relating to the terminal comprises the readiness of the terminal to receive a notification message indicating that a message addressed to the terminal has been stored.

27. A server according to claim 13, wherein the server is configured to send a notification message to the terminal requesting that the terminal become able to receive multimedia messages.

28. A computer program product according to claim 15, wherein the program code for causing said server to send an inquiry to the cellular network comprises program code for causing said server to send an inquiry to a gateway element of the cellular network.

29. A computer program product according to claim 28, wherein the gateway element is a 3G-GGSN.

30. A computer program product according to claim 15, wherein the program code for causing said server to send an inquiry to the cellular network comprises program code for causing said server to send an inquiry to a first element of the cellular network, and wherein program code for causing said server to receive a response message comprises program code for causing said server to receive the response message from the first element of the cellular network.

31. A computer program product according to claim 15, wherein the information relating to the terminal comprises the readiness of the terminal to receive data.

32. A computer program product according to claim 15, further comprising program code for repeating the inquiry as a result of a response message indicating the terminal is not ready to receive data.

33. A computer program product according to claim 15, wherein said first identifier comprises:

a first part that indicates a messaging service subscriber; and

a second part that indicates the server.

34. A computer program product according to claim 15, wherein the information relating to the terminal comprises the readiness of the terminal to receive a notification message indicating that a message addressed to the terminal has been stored.

35. A computer program product according to claim 15, further comprising program code for sending a notification message to the terminal requesting that the terminal become able to receive multimedia messages.

36. A network element according to claim 16, wherein said second identifier is one of the following: an IMSI (International Mobile Subscriber Identity) code, and IMUI (International Mobile User Identity) code.

37. A network element according to claim 16, wherein the network element is a 3G-GGSN.

38. A network element according to claim 16, wherein the information relating to a terminal comprises information regarding whether the terminal is attached to the cellular network.

39. A network element according to claim 16, wherein the information relating to the terminal comprises the readiness of the terminal to receive data.

40. A network element according to claim 16, wherein the network element is a gateway element of the cellular network.

41. A network element according to claim 16, wherein the means for mapping are configured to map the first identifier to the second identifier by consulting a second element.

42. A network element according to claim 41, wherein said first identifier comprises:

a first part that indicates a messaging service subscriber; and

a second part that indicates the server.

43. A network element according to claim 41, wherein the second element is a Domain Name Server.

44. A network element according to claim 41, wherein the second element is a Home Location Register.

45. A network element according to claim 16, wherein the response message does not include an IP address of the terminal.

46. A network element according to claim 16, wherein the response message includes an IP address of the terminal.

47. A network element according to claim 16, wherein the means for determining are configured to determine the readiness of the terminal to receive data via the network element.

48. A network element according to claim 47, wherein the means for determining are configured to determine, as a result of determining the terminal is not ready to receive data via the network element, whether the terminal is ready to receive data via another element.

49. The network element of claim 48, wherein the means for determining are configured to obtain, after determining the terminal is not ready to receive data via the network element and before determining whether the terminal is ready to receive data via another element, a list of nodes in the cellular network to which the terminal can connect.

50. The network element of claim 16, wherein the network element is configured to obtain an IP address of the terminal.

51. The network element of claim 16, wherein the response message comprises an address of a second element of the cellular network and an indication that the terminal is ready to receive data via the second element.

52. The network element of claim 16, wherein the means for determining are configured consult a second element for information regarding whether the terminal is ready to receive data.

53. The network element of claim 52, wherein the means for determining are configured to receive an identification of the second element by sending an information request message to a third element.

54. A network element of claim 16, wherein the cellular network includes the network element, a second element, a third element and a fourth element, and wherein

the means for determining are configured to send a first cellular network message to the second element,

the second element is configured to send, as a result of the first cellular network message, a second cellular network message to the third element,

the third element is configured to send a third cellular network message to the second element as a result of the second cellular network message, the third cellular network message identifying the fourth element,

the second element is configured to send a fourth cellular network message to the network element as a result of the third cellular network message, the fourth cellular network message comprising information identifying the fourth element, and

the response message includes information identifying the fourth element.

55. A network element of claim 16, wherein the cellular network includes the network element, a second element, a third element and a fourth element, and wherein

the means for determining are configured to send a first cellular network message to the second element,

the second element is configured to send a second cellular network message to the network element as a result of the first cellular network message, the second cellular network message comprising information identifying the third element,

the network element is configured to send a third cellular network message to the third element as a result of the second cellular network message,

the third element is configured to send a fourth cellular network message to the network element as a result of the third cellular network message, the fourth cellular network message comprising information identifying the fourth element, and

the response message includes information identifying the fourth element.

56. A network element of claim 16, wherein the response message indicates that multimedia messaging to the terminal is not permitted.

57. The network element of claim 56, wherein the network element is configured to determine, prior to sending the response message, that bills associated with the terminal have not been paid.

58. A network element according to claim 16, wherein the information relating to the terminal comprises the readiness of the terminal to receive a notification message indicating that a message addressed to the terminal has been stored.

59. A computer program product according to claim 18, wherein said second identifier is one of the following: an IMSI (International Mobile Subscriber Identity) code, and IMUI (International Mobile User Identity) code.

60. A computer program product according to claim 18, wherein the network element is a 3G-GGSN.

61. A computer program product according to claim 18, wherein the information relating to a terminal comprises information regarding whether the terminal is attached to the cellular network.

62. A computer program product according to claim 18, wherein the information relating to the terminal comprises the readiness of the terminal to receive data.

63. A computer program product according to claim 18, wherein the network element is a gateway element of the cellular network.

64. A computer program product according to claim 18, further comprising program code for causing the network element to map the first identifier to the second identifier by consulting a second element.

65. A computer program product according to claim 64, wherein said first identifier comprises:

a first part that indicates a messaging service subscriber; and

a second part that indicates the server.

66. A computer program product according to claim 64, wherein the second element is a Domain Name Server.

67. A computer program product according to claim 64, wherein the second element is a Home Location Register.

68. A computer program product according to claim 18, wherein the response message does not include an IP address of the terminal.

69. A computer program product according to claim 18, wherein the response message includes an IP address of the terminal.

70. A computer program product according to claim 18, comprising further program code for causing the network element to determine said information by determining the readiness of the terminal to receive data via the network element.

71. A computer program product according to claim 70, comprising further program code for causing the network element to determine, as a result of determining the terminal is not ready to receive data via the network element, whether the terminal is ready to receive data via another element.

72. A computer program product according to claim 71, comprising further program code for causing the network element to obtain, after determining the terminal is not ready to receive data via the network element and before determining whether the terminal is ready to receive data via another element, a list of nodes in the cellular network to which the terminal can connect.

73. A computer program product according to claim 18, comprising further program code for causing the network element to obtain an IP address of the terminal.

74. A computer program product according to claim 18, wherein the response message comprises an address of a second element of the cellular network and an indication that the terminal is ready to receive data via the second element.

75. A computer program product according to claim 18, comprising further program code for causing the network element to consult a second element for information regarding whether the terminal is ready to receive data.

76. A computer program product according to claim 75, comprising further program code for causing the network element to receive an identification of the second element by sending an information request message to a third element.

77. A computer program product according to claim 18, wherein the response message indicates that multimedia messaging to the terminal is not permitted.

78. A computer program product according to claim 77, comprising further program code for causing the network element to determine, prior to sending the response message, that bills associated with the terminal have not been paid.

79. A computer program product according to claim 18, wherein the information relating to the terminal comprises the readiness of the terminal to receive a notification message indicating that a message addressed to the terminal has been stored.

80. A system according to claim 19, wherein the server is configured to repeat the inquiry as a result of a response message indicating the terminal is not ready to receive data.

81. A system according to claim 19, wherein said first identifier comprises:

a first part that indicates a messaging service subscriber; and

a second part that indicates the server.

82. A system according to claim 19, wherein the server is configured to

send the inquiry to network element, and

receive in the response an address of a second element of the cellular network and an indication that the terminal is ready to receive data via the second element.

83. A system according to claim 19, wherein the server is configured to send a notification message to the terminal requesting that the terminal become able to receive multimedia messages.

84. A system according to claim 19, wherein said second identifier is one of the following: an IMSI (International Mobile Subscriber Identity) code, and IMUI (International Mobile User Identity) code.

85. A system according to claim 19, wherein the network element is a 3G-GGSN.

86. A system according to claim 19, wherein the information relating to a terminal comprises information regarding whether the terminal is attached to the cellular network.

87. A system according to claim 19, wherein the information relating to the terminal comprises the readiness of the terminal to receive data.

88. A system according to claim 19, wherein the network element is a gateway element of the cellular network.

89. A system according to claim 19, wherein the means for mapping are configured to map the first identifier to the second identifier by consulting a second element.

90. A system according to claim 89, wherein said first identifier comprises:

a first part that indicates a messaging service subscriber; and

a second part that indicates the server.

91. A system according to claim 89, wherein the second element is a Domain Name Server.

92. A system according to claim 89, wherein the second element is a Home Location Register.

93. A system according to claim 19, wherein the response message does not include an IP address of the terminal.

94. A system according to claim 19, wherein the response message includes an IP address of the terminal.

95. A system according to claim 19, wherein the means for determining are configured to determine the readiness of the terminal to receive data via the network element.

96. A system according to claim 95, wherein the means for determining are configured to determine, as a result of determining the terminal is not ready to receive data via the network element, whether the terminal is ready to receive data via another element.

97. A system according to claim 96, wherein the means for determining are configured to obtain, after determining the terminal is not ready to receive data via the network element and before determining whether the terminal is ready to receive data via another element, a list of nodes in the cellular network to which the terminal can connect.

98. A system according to claim 19, wherein the network element is configured to obtain an IP address of the terminal.

99. A system according to claim 19, wherein the response message comprises an address of a second element of the cellular network and an indication that the terminal is ready to receive data via the second element.

100. A system according to claim 19, wherein the means for determining are configured consult a second element for information regarding whether the terminal is ready to receive data.

101. A system according to claim 100, wherein the means for determining are configured to receive an identification of the second element by sending an information request message to a third element.

102. A system according to claim 19, wherein the cellular network includes the network element, a second element, a third element and a fourth element, and wherein

the means for determining are configured to send a first cellular network message to the second element,

the second element is configured to send, as a result of the first cellular network message, a second cellular network message to the third element,

the third element is configured to send a third cellular network message to the second element as a result of the second cellular network message, the third cellular network message identifying the fourth element,

the second element is configured to send a fourth cellular network message to the network element as a result of the third cellular network message, the fourth cellular network message comprising information identifying the fourth element, and

the response message includes information identifying the fourth element.

103. A system according to claim 19, wherein the cellular network includes the network element, a second element, a third element and a fourth element, and wherein

the means for determining are configured to send a first cellular network message to the second element,

the second element is configured to send a second cellular network message to the network element as a result of the first cellular network message, the second cellular network message comprising information identifying the third element,

the network element is configured to send a third cellular network message to the third element as a result of the second cellular network message,

the third element is configured to send a fourth cellular network message to the network element as a result of the third cellular network message, the fourth cellular network message comprising information identifying the fourth element, and

the response message includes information identifying the fourth element.

104. A system according to claim 19, wherein the response message indicates that multimedia messaging to the terminal is not permitted.

105. A system according to claim 104, wherein the network element is configured to determine, prior to sending the response message, that bills associated with the terminal have not been paid.

106. A system according to claim 19, wherein the information relating to the terminal comprises the readiness of the terminal to receive a notification message indicating that a message addressed to the terminal has been stored.

107. A server external to a cellular network for inquiring about specific information, relating to a terminal of the cellular network, from the cellular network, wherein the server comprises:

means for defining a specific first identifier external to the cellular network for identifying said terminal;

means for sending an inquiry from the server to the cellular network, the inquiry comprising said first identifier to be mapped in the cellular network to a specific second identifier so as to determine said information relating to the terminal with the aid of said second identifier, and wherein said second identifier is an internal identifier of the cellular network; and

means for receiving a response message sent from the cellular network in response to said inquiry, the response message comprising said determined information relating to said terminal, indicated with the aid of said first identifier, and wherein the server is configured to

send the inquiry to a first element of the cellular network, and

receive in the response an address of a second element of the cellular network and an indication that the terminal is ready to receive data via the second element.

108. A computer program product executable in a server external to a cellular network for inquiring about specific information, relating to a terminal of the cellular network, from the cellular network, wherein the computer program product comprises:

program code for defining a first identifier external to the cellular network for identifying said terminal;

program code for causing said server to send an inquiry to the cellular network by causing said server to send an inquiry to a first element of the cellular network, the inquiry comprising said first identifier to be mapped in the cellular network to a specific second identifier so as to determine said information relating to the terminal with the aid of said second identifier, and wherein said second identifier is an internal identifier of the cellular network;

program code for causing said server to receive a response message sent from the cellular network in response to said inquiry, the response message comprising said determined information relating to said terminal, indicated with the aid of said first identifier; and

program code for receiving in the response an address of a second element of the cellular network and an indication that the terminal is ready to receive data via the second element.

109. A network element of a cellular network, comprising:

means for receiving an inquiry sent by a server external to the cellular network, the inquiry comprising a request to determine specific information relating to a terminal of the cellular network, and the inquiry comprising a first identifier for identifying said terminal, the first identifier being a specific identifier external to the cellular network;

means for mapping said first identifier to a specific second identifier, the second identifier being an internal identifier of the cellular network;

means for determining said information relating to the terminal with the aid of said second identifier; and

means for sending a response message to the server external to the cellular network in response to said inquiry, the response message comprising the information relating to said terminal indicated with the aid of said first identifier, and

wherein the network element is configured to not reveal the second identifier to the server.

110. A computer program executable in a network element of a cellular network, wherein the computer program product comprises program code:

for causing the network element to receive an inquiry sent by a specific server external to the cellular network, the inquiry comprising a request to determine specific information relating to a terminal of the cellular network, and the inquiry comprising a first identifier for identifying said terminal, the first identifier being a specific identifier external to the cellular network;

for mapping said first identifier to a specific second identifier, the second identifier being an internal identifier of the cellular network;

for causing the network element to determine said information relating to the terminal with the aid of said second identifier;

for causing the network element to send a response message to the server external to the cellular network in response to said inquiry, the response message com-

prising the information relating to said terminal indicated with the aid of said first identifier; and

for causing the network element to not reveal the second identifier to the server.

111. A system comprising a server external to a cellular network and a network element of the cellular network for inquiring about information, relating to a terminal of the cellular network from the cellular network from the server external to the cellular network, wherein the server comprises:

means for defining a specific first identifier external to the cellular network for identifying said terminal;

means for sending an inquiry from the server to the network element of the cellular network to determine said information relating to the terminal, the inquiry comprising said first identifier and that the network element of the cellular network comprises:

means for receiving said inquiry;

means for mapping said first identifier to a specific second identifier, the second identifier being an internal identifier of the cellular network;

means for determining said information relating to the terminal with the aid of said second identifier; and

means for sending a response to the server external to the cellular network in response to said inquiry, the response message comprising the information relating to said terminal indicated with the aid of said first identifier, and

wherein the network element is configured to not reveal the second identifier to the server.

112. A method for inquiring about information relating to a wireless terminal of a cellular network, from the cellular network by a messaging server external to the cellular network, wherein the method comprises:

sending an inquiry from the messaging server to the cellular network to determine said information relating to the terminal, the inquiry comprising a first identifier identifying said terminal, the first identifier being a specific identifier external to the cellular network;

mapping said first identifier to a specific second identifier in the cellular network, the second identifier being an internal identifier of the cellular network, wherein the mapping is not performed by a Home Location Register;

determining said information relating to the terminal with the aid of said second identifier; and

sending a response message in response to said inquiry from the cellular network to said messaging server external to the cellular network, in which response message the information relating to said terminal is indicated with the aid of said first identifier.

113. The method of claim 112, wherein the inquiry is sent to, and the determining is performed by, the same element of the cellular network.

* * * * *

UNITED STATES PATENT AND TRADEMARK OFFICE

CERTIFICATE OF CORRECTION

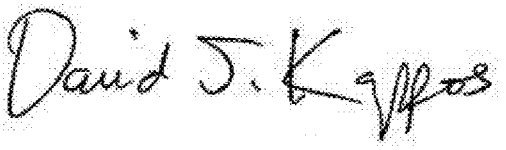
PATENT NO.	: 6,885,870 B2
APPLICATION NO.	: 09/745756
DATED	: April 26, 2005
INVENTOR(S)	: Outi Aho

It is certified that error appears in the above-identified patent and that said Letters Patent is hereby corrected as shown below:

On the cover page, "Field" item (22):
replace "Feb. 22, 2001" with --Dec. 21, 2000--

On the cover page of the EX PARTE REEXAMINATION CERTIFICATE (8597th), opposite the word "Filed" under the "Reexamination Certificate for" section:
replace "Feb. 22, 2001" with --Dec. 21, 2000--

Signed and Sealed this
Thirteenth Day of March, 2012



David J. Kappos
Director of the United States Patent and Trademark Office

EXHIBIT B

US005987323A

United States Patent [19]

Huotari

[11] Patent Number: 5,987,323

[45] Date of Patent: Nov. 16, 1999

[54] **STARTING A SHORT MESSAGE TRANSMISSION IN A CELLULAR COMMUNICATION SYSTEM**

[75] Inventor: **Seppo Huotari**, Espoo, Finland

[73] Assignee: **Nokia Telecommunications OY**, Espoo, Finland

[21] Appl. No.: **08/776,071**

[22] PCT Filed: **Jul. 17, 1995**

[86] PCT No.: **PCT/FI95/00405**

§ 371 Date: **Apr. 1, 1997**

§ 102(e) Date: **Apr. 1, 1997**

[87] PCT Pub. No.: **WO96/03843**

PCT Pub. Date: **Feb. 8, 1996**

[30] **Foreign Application Priority Data**

Jul. 20, 1994 [FI] Finland 943447

[51] **Int. Cl.**[6] **H04B 7/26**

[52] **U.S. Cl.** **455/433**; 455/466

[58] **Field of Search** 455/422, 432, 455/433, 435, 458, 466, 462, 517, 518, 521, 414

[56] **References Cited**

U.S. PATENT DOCUMENTS

5,794,142	8/1998	Vanttila et al.	455/466
5,806,000	9/1998	Vo et al.	455/466

FOREIGN PATENT DOCUMENTS

94/07338	3/1994	WIPO .
95/12933	5/1995	WIPO .

OTHER PUBLICATIONS

ETSI–GSM Technical Specification, GSM 03.40 Version 3.5.0, European digital cellular telecommunication system (phase 1); "Technical Realization of the Short Message Service—Point–to Point", 1992, pp. 13–15.

ITG–Fachbericht 124, Informationstechnische Gesellschaft Fachtagung, Mobile Kommunikation,Vortrage der ITG–Fachtagung, Sep. 27–29, 1993 in Neu–Ulm, vde–verlag gmbh, Berlin, Hientz, Michael et al : "Der short message service—ein neuer dienst der digitalen mobilkommunikation " pp. 517–526.

ETSI/TC GSM, "Recommendation GSM 01.02, General Description of a GSM PLMN", Mar. 1990.

ETSI/TC GSM, "Report GSM 11.30, Mobile services Switching Centre", Jan. 1990.

ETSI/TC GSM, "Report GSM 11.31, Home Location Register Specification", Jan. 1990.

ESTI/TC GSM, "Report GSM 11.32, Visitor Location Register Specification", Jan. 1990.

ETSI TC–SMG, European digital cellular telecommunications system (Phase 2); Technical realization of the short Message Service (SMS) Point to Point (PP) (GSM 03.40), Oct. 1993.

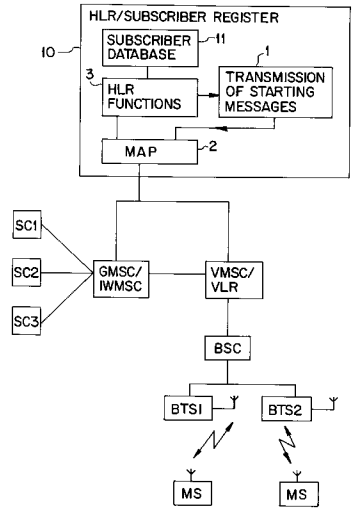
Primary Examiner—Thanh Cong Le

Attorney, Agent, or Firm—IP Group of Pillsbury Madison & Sutro LLP

[57] **ABSTRACT**

A method for starting a short message transmission in a cellular communication system, a cellular communication system, and a cellular communication system subscriber location register includes the subscriber location register which stores information on the fact that at least one short message service center stores short messages to be transmitted to a subscriber to whom the messages cannot be transmitted for the time being, and the subscriber location register of the subscriber which transmits to at least one short message service center a short message transmission starting message when it is again possible to transmit short messages to the subscriber. In order that short messages can be transmitted to subscribers selectively, the subscriber location register maintains short message service center and subscriber-specific information on the conditions under on which the short message service center is to be transmitted short message transmission starting messages.

14 Claims, 3 Drawing Sheets



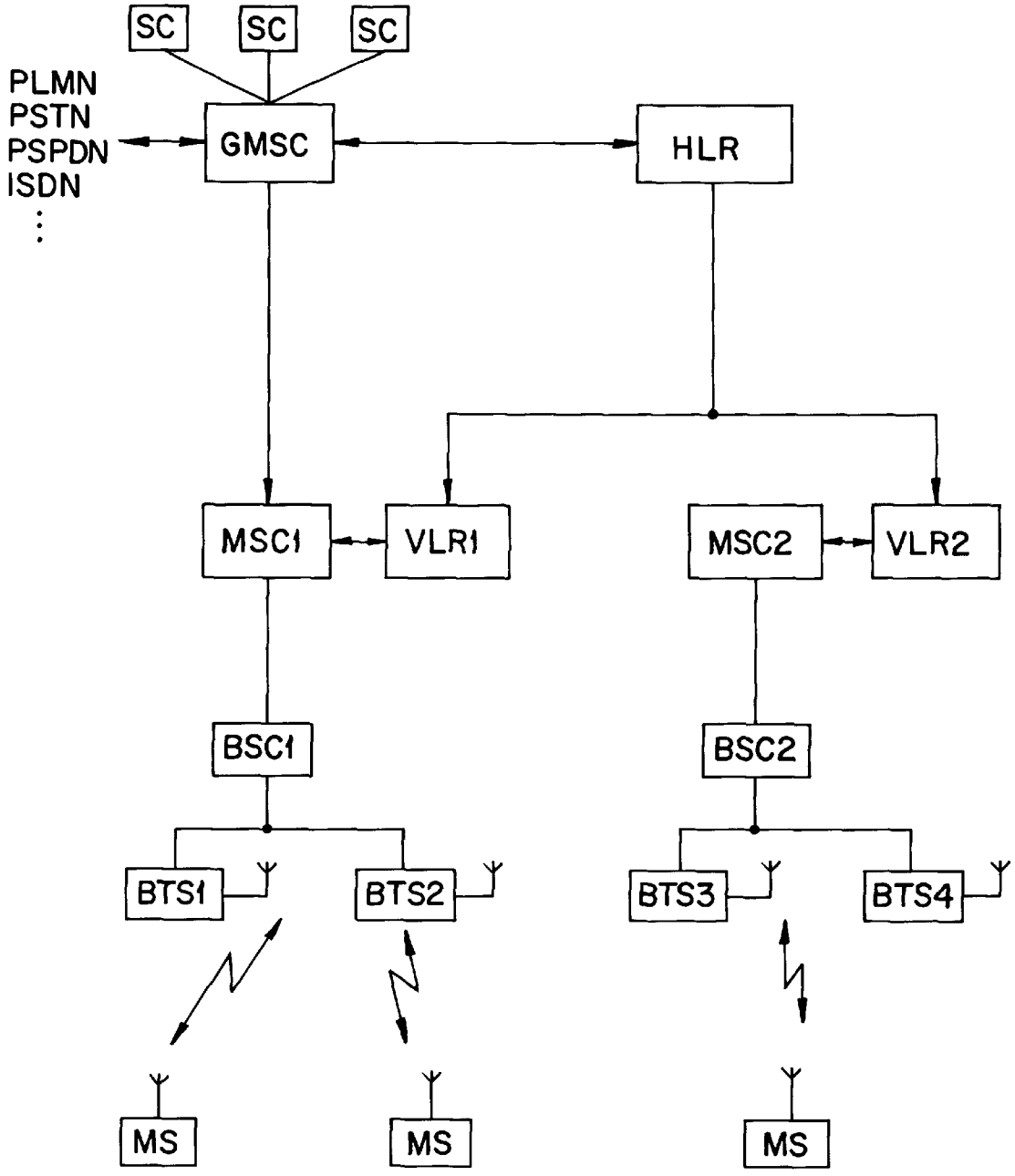

SC
SC
SC
PLMN
PSTN
PSPDN
ISDN
GMSC
HLR
MSC1
VLR1
MSC2
VLR2
BSC1
BSC2
BTS1
BTS2
BTS3
BTS4
MS
MS
MS

FIG. 1

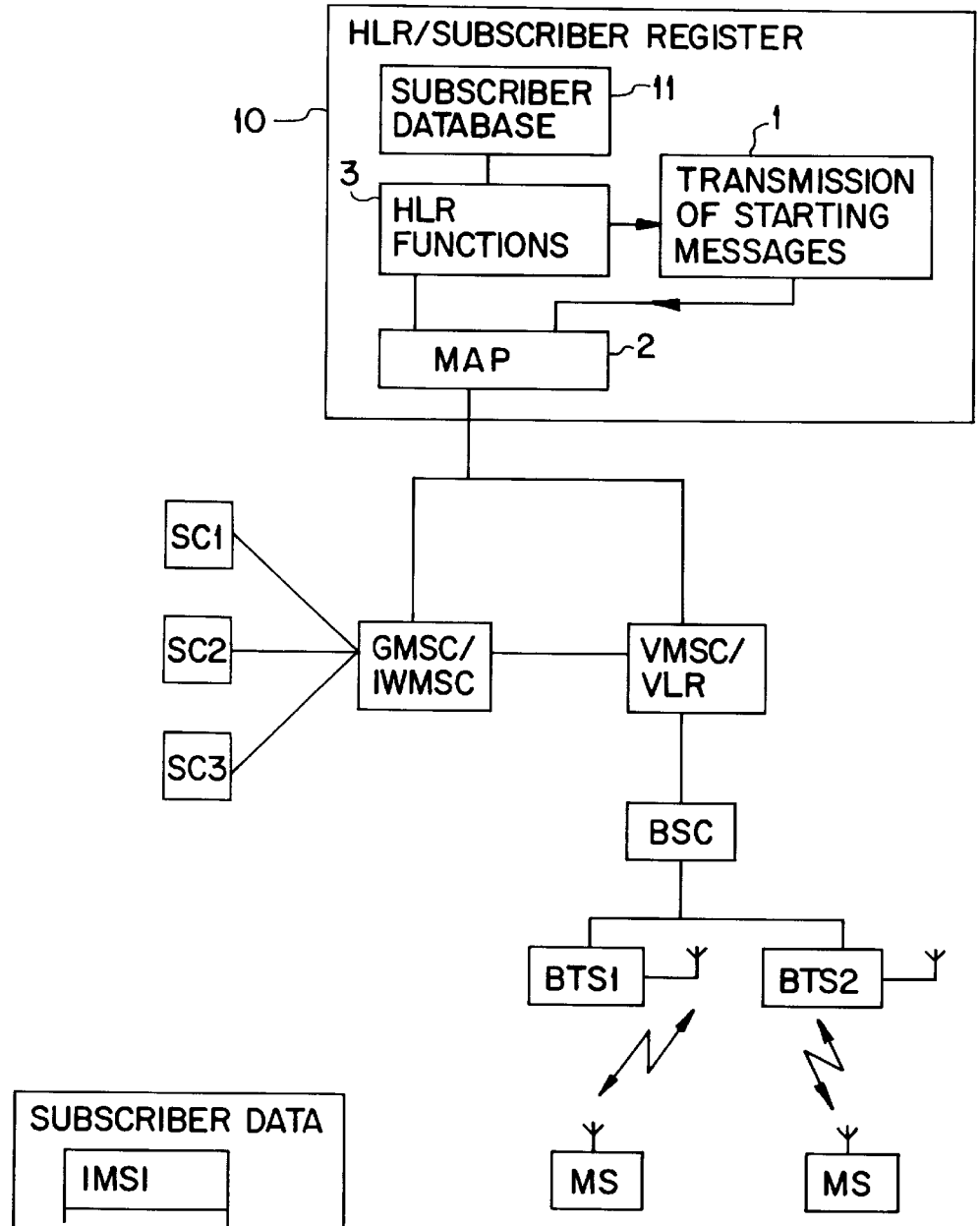

HLR/SUBSCRIBER REGISTER
SUBSCRIBER DATABASE
11
10
1
3
HLR FUNCTIONS
TRANSMISSION OF STARTING MESSAGES
MAP
2
SC1
SC2
SC3
GMSC/ IWMSC
VMSC/ VLR
BSC
BTS1
BTS2
MS
MS

FIG. 3

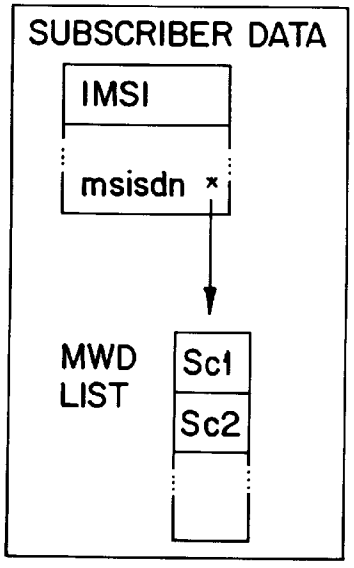

SUBSCRIBER DATA
IMSI
msisdn
MWD LIST
Sc1
Sc2

FIG. 2

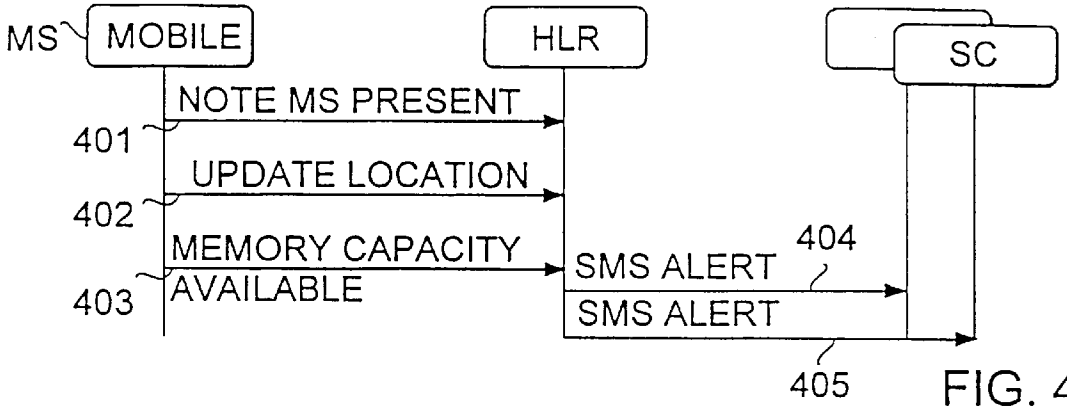


FIG. 4

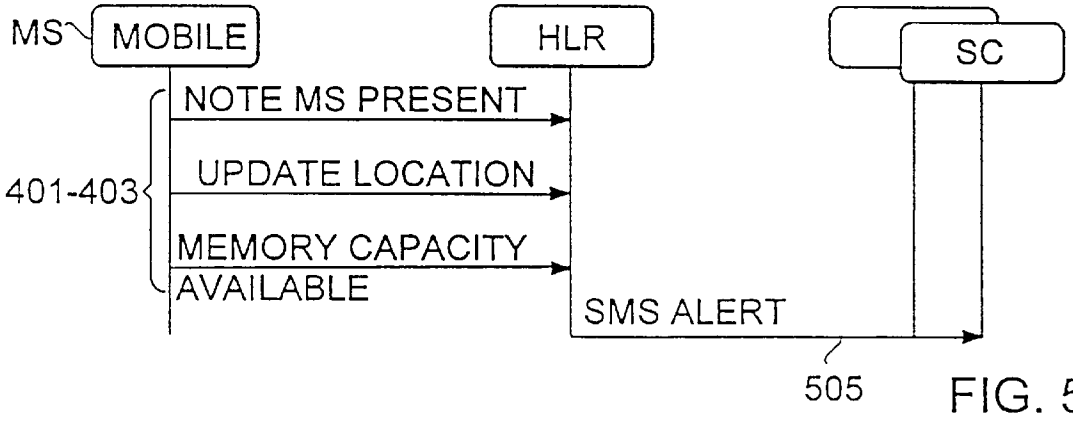


FIG. 5

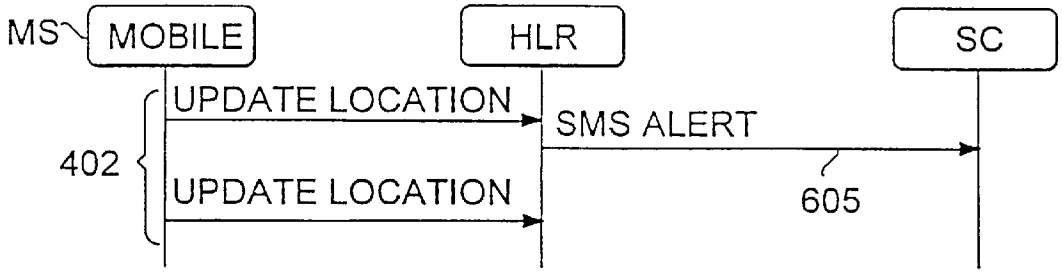


FIG. 6

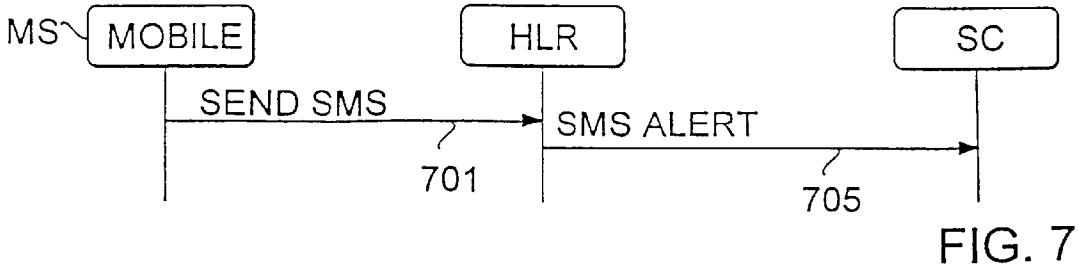


FIG. 7

STARTING A SHORT MESSAGE TRANSMISSION IN A CELLULAR COMMUNICATION SYSTEM

This application is the national phase of international application PCT/FI95/00405 filed Jul. 17, 1995 which designated the U.S.

FIELD OF THE INVENTION

The present invention relates to a method for starting a short message transmission in a cellular communication network, a corresponding cellular communication system, and a cellular communication system subscriber location register. In this method, the subscriber location register stores information based on the fact that at least one short message service center stores short messages to be transmitted to a subscriber, to whom these messages cannot be transmitted for the time being, and the subscriber location register of the subscriber transmits to the at least one short message service center, a short message transmission starting message, when it is again possible to transmit short messages to the subscriber.

BACKGROUND OF THE INVENTION

Today, different cellular communication or mobile telephone systems are used and planned in which the geographical area covered by a system is divided into smaller separate radio areas, i.e., cells, so that when located in a cell, a radio phone or a mobile phone communicates with the fixed network via the fixed radio station located in the cell. The mobile phones included in the system may freely move within the system area from a cell into another. One of these systems is the digital mobile phone system GSM (Global System for Mobiles).

As to cellular communication networks, it is known practice to transmit short messages via a short message service center separate from the cellular communication network. One of these systems for transmitting and forwarding short messages is described in ETSI GSM system recommendation "GSM 03.40, February 1992, Technical Realization of Short Message Services Point to Point, ETSI/PT". It describes the connection of a short message service center to the mobile exchange of a cellular communication network and the operation of this short message service center when the center transmits and forwards short messages from outside the cellular communication network and from a cellular communication network subscriber (subscriber A) to another network subscriber (subscriber B), or to a means of communication which is capable of receiving and/or transmitting short messages and which is located outside the network.

When a short message service center attempts to transmit a short message to a subscriber B. and the subscriber B is not reachable, a Messages-Waiting-Data-List according to GSM recommendation 03.40, i.e., an MWD list, is established in the home location register, which stores a list, subscriber B-specific, of the addresses of those short message service centers which store short messages to be delivered to subscribers B. Accordingly, when subscriber B registers in the network, i.e., it is possible to transmit a short message to the mobile phone of the subscriber B since the visitor location register in the area which subscriber B registers itself transmits a notification of the arrival of the subscriber B in the network to the home location register of the subscriber B. The home location register of the subscriber B, i.e., the subscriber location register, thus starts to transmit

notifications, i.e., short message transmission starting messages, or, Alert messages (Alert), to the short message service centers presented in the Messages-Waiting-Data-List of the subscriber. The starting messages inform the short message service centers that subscriber B has become active in the cellular communication network area and that it is worth attempting to transmit a short message to the mobile phone of subscriber B. A situation of this type may occur, for instance, when the subscriber has switched off her mobile phone for the night and switches it on in the morning, or correspondingly, if the subscriber uses a mobile phone at work and switches on her mobile phone at the beginning of working hours.

A typical problem of prior art solutions is that the transmission capacity of short messages from short message service centers to a subscriber is very restricted. The transmission capacity on the radio path is only 10–100 bytes/second, which is significantly less than what is used, for instance, in modem communication between computers. However, it has been required that short message transmissions should be capable of forwarding even electronic mail-type messages to subscribers. The transmission capacity of short messaged is typically a crucial characteristic in the situations described above. Thus, when a subscriber B has suddenly become reachable, attempts are made to transmit to subscriber B a large number of short messages, which have been stored in possibly several short message service centers. The short messages suddenly transmitted to the subscriber thus congest the short message reception of the subscriber, i.e., the mobile phone, and possibly also the transmission link or radio path to the subscriber. As a result of the congestion, a new and possibly urgent short message for the subscriber may not reach its destination quickly enough because the short message reception of the subscriber, i.e., the mobile phone, is congested. Important short messages are thus lost, in a manner of speaking, in the multitude of less important, queuing short messages.

Another problem of prior art solutions, which occurs when short messages can be transmitted again to the subscriber B after a pause, is that the short messages intended for subscriber B arrive in succession to subscriber B and disturb the user of the subscriber station with their arrival and possible audio signals connected to the arrival for a very long time, i.e., as long as the subscriber has short messages to receive. This disturbing period may last for an extremely long time due to the low transmission speed of the short message-transmitting radio path, according to the GSM specification, and to the fact that the subscriber has to receive all short messages. The aggravation of the subscriber is naturally added to by the fact that the subscriber has no possibility of selecting from the short messages those short messages the transmitters, i.e., short message service centers, of which said subscriber considers the most important.

Yet another problem of prior art solutions is that subscriber B cannot select or eliminate arriving short messages in a desired manner, but must receive all the short messages transmitted to it.

One prior art method for starting a short message transmission in a cellular communication system, a cellular communication system, and a cellular communication system subscriber location register has been disclosed in Finnish Patent Application 924,198, which corresponds to International Patent Application PCT/FI93/00373.

SUMMARY OF THE INVENTION

An object of the present invention is to obviate a problem caused by an insufficient transmission capacity in transmit-

ting short messages from short message service centers to subscribers and by the fact that the short messages transmitted to a subscriber are congested when the subscriber has suddenly entered a state in which it can be transmitted short messages. In addition to this, a problem is caused by the fact that important short messages to be delivered to the subscribers remain undelivered or arrive too late because they are transmitted only when the subscriber has received the congested short messages, which were transmitted first.

In addition to the above, an object of the invention is to obviate a problem caused by the fact that the subscriber cannot select the short messages transmitted to him and cannot thus limit the number of the short messages transmitted to him.

Furthermore, an object of the invention is to ensure that important short messages reach their destination even when there are suddenly a large number of short messages to be transmitted to the subscriber.

In this method for starting a short message transmission in a cellular communication system, information on the conditions on which the short message service center is transmitted short message transmission starting messages is maintained at that specific to the short message service center and to the subscriber in the subscriber location register.

The cellular communication system of the present invention includes a subscriber; at least one short message service center which transmits short messages to the subscriber via the cellular communication network and which stores short messages when the subscriber is not reachable; the subscriber location register of the subscriber contains information on the fact that the at least one short message service center stores short messages to be transmitted to the unreachable subscriber, the subscriber location register including a transmitter which transmits a short message transmission starting message to the at least one short message service center when it is possible again to transmit short messages to the subscriber.

In the cellular communication system of the invention, the subscriber location register includes a database, in which information on the conditions on which the short message service center is transmitted short message transmission starting messages is maintained specific to the short message service center and to the subscriber.

The subscriber location register of a cellular communication system of the present invention includes a transmitter which transmits a short message transmission starting message to at least one short message service center. The subscriber location register of the invention includes a database, in which information on the conditions on which the short message service center is transmitted short message transmission starting messages is maintained specific to the short message service center and to the subscriber.

The invention is based on the idea that in the subscriber location register of the cellular communication system, for instance, in a home location register (HLR), information is maintained in a database on the conditions, i.e., when, in which order, and for the subscriber situated in which location, on which a short message service center storing short messages intended for the subscriber is transmitted short message transmission starting messages, i.e., Alert messages. This brings about a situation where the subscriber location register transmits the short message transmission starting messages, i.e., Alert messages, concerning a particular subscriber B. i.e., the receiver, to those short message service centers which are actually desired to transmit short messages to subscriber B. Starting messages are selectively transmitted to short message service centers based on the maintained information so that starting messages are transmitted to only those (first) short message service centers which are desired to transmit short messages. Correspondingly, starting messages are not transmitted to those (second) short message service centers which are not desired to transmit short messages, even if those (second) short message service centers contain short messages to be transmitted to subscriber B. The invention prioritizes the transmission of short message transmission starting messages so that when it is possible to transmit short messages to a subscriber after a pause, the subscriber is first transmitted important starting messages only.

An advantage of this method for starting a short message transmission in a cellular communication system, cellular communication system, and cellular communication system subscriber location register is that the congestion of short messages on the radio path when it is possible again to start transmitting short messages to a subscriber after a pause is prevented.

Another advantage of the invention is that it is possible to avoid a situation where the mobile station of a subscriber has to receive, in succession, a large number of short messages stored in the network with the result that the user of the -subscriber station is disturbed and gets weary of large number of short messages in receiving a succession.

Yet another advantage of the invention is that it enables a subscriber to select those short messages which the subscriber desires to receive at her own subscriber station, i.e., mobile station.

A further advantage of the invention is that it provides a subscriber B who is receiving short messages, with the ability to restrict the number of the short messages received, for instance, based on which short message service center has transmitted or forwarded the short message.

Furthermore, an advantage of the invention is that it offers a subscriber the ability to divide short messages based on her own geographical location into those which the subscriber desires to receive within a certain period of time, and correspondingly, into those which the subscriber does not want to receive.

BRIEF DESCRIPTION OF THE FIGURES

In the following, the invention will be described in more detail with reference to the accompanying drawings, in which

FIG. **1** is a schematic illustration of a cellular communication system in which the method and mobile exchange of the invention can be used;

FIG. **2** shows the hierarchy of the subscriber data of a subscriber home location register, i.e., a subscriber location register;

FIG. **3** shows a block diagram of the cellular communication system of the invention and the subscriber location register thereof;

FIG. **4** shows a signaling diagram of a situation where a subscriber has become reachable, and only part of the short message transmission starting messages are transmitted;

FIG. **5** shows a signaling diagram of a situation where a subscriber has become reachable, and short message transmission starting messages are transmitted to only certain short message service centers,

FIG. **6** shows a signaling diagram of a situation where a subscriber has become reachable, and short message trans-

mission starting messages are transmitted to only certain short message service centers, depending on the subscriber's location; and

FIG. **7** shows a signaling diagram of a situation where a subscriber requests and controls the transmission of short message transmission starting messages.

DETAILED DESCRIPTION OF THE INVENTION

In the following, the method of the invention will be described as applied in the digital GSM mobile telephone system, which is the preferred field of application of the invention. The method of the invention can, however, also be applied in other radio systems of a similar type or in adaptations of the GSM system. The basic structure and facilities of the GSM mobile telephone system are known to ones skilled in the art and defined relatively precisely in the GSM system specifications, especially in "GSM Recommendations 01.02; 11.30; 11.31; 11.32; and 03.40".

A GSM network, which is shown in FIG. **1**, usually comprises one home location register HER, which is a database in which the data of a mobile phone, such as the location data, is permanently stored. The home location register performs basically the same tasks as the subscriber location register of the invention. The system also comprises several visitor location registers VLR, of which there are one or more for one exchange area. A visitor location register VLR is a database in which the data of a mobile phone is stored for the period that the mobile phone visits the VLR area, i.e., the location area of the mobile phone. The VLR knows the location of the mobile phone MS with an accuracy of one location area As for the HLR, it knows which VLR the mobile phone MS is visiting and gives mobile phone MS—terminating calls routing information to the telephone network, i.e., the VLR address of the location area of the subscriber B. The HLR obtains the necessary routing information from the VLR. The HLR and VLR have only a signaling connection with the other components of the mobile telephone network. In the system according to FIG. **1**, each exchange area has its own visitor location register VLR, which is connected to the mobile or radio telephone exchange MSC of the exchange area. In the solution shown in the figure, two exchange areas are illustrated, one comprising a mobile exchange MSC**1** and a visitor location register VLR**1**, and the other comprising a mobile exchange MSC**2** and a visitor location register VLR**2**. Under both exchange areas, there are one or more location areas, and in each location area, the traffic is controlled by a base station controller (BSC), which controls several fixed radio stations, i.e., base transceiver stations (BTS). Each of the above-mentioned radio cells comprises one base station BTS, and one base station controller BSC serves several cells. A mobile phone MS located in a cell establishes a two-way radio connection with the base transceiver station BTS of said cell. There are both a signaling connection and speech channels between the base station controller BSC and the mobile exchange MSC. Correspondingly, under the other exchange area MSC**2** is a location area with a base station controller BSC**2** and base stations BTS**3** and BTS**4**.

A GSM network is usually connected to other networks, such as a public-switched telephone network PSTN, another mobile telephone network PLMN, a packet-switched public data network PSPDN or, an ISDN network ISDN or short message service center SC, via a certain mobile exchange referred to as a gateway exchange GMSC. One or more (all) mobile exchanges of the network can act as a gateway exchange GMSC. From the gateway exchange GMSC, it is possible to switch a speech channel connection to any other mobile exchange MSC of the network. The gateway exchange GMSC also has a signaling connection with the home location register HLR. The home location register HLR has a signaling connection with the visitor location registers VLR. Alternatively, an exchange of another data transmission system, for instance an ISDN exchange, can also act as a gateway exchange. FIG. **1** also shows several short message service centers SC, which transmit a short message via the cellular communication network to the mobile phone MS of the subscriber B and which, during the time the subscriber is not reachable, store the short messages intended to be transmitted later to the subscriber.

FIG. **2** shows the hierarchy of the subscriber data of a subscriber home location register, i.e., a subscriber location register. The subscriber data is stored based on the subscriber's international mobile subscriber identity IMSI in the home location register of the subscriber as subscriber-specific records, which stores the supplementary services ordered by the subscriber in addition to the basic service of the subscriber. The basic services of a subscriber are the normal telephone service, short message transmission and reception services, and different data transmission services. The supplementary services of a subscriber include, for instance, call forwarding and call restriction services, and call waiting service. One basic service of the subscriber can correspond to one MSISDN number, msisdn of the subscriber, i.e., the "directory number" of a certain teleservice of the subscriber. In the GSM system, it is possible to transmit short messages to a subscriber based on any directory number, i.e., the corresponding basic service of the subscriber, or, the MSISDN number, of the same subscriber. Each MSISDN number of the subscriber and the basic service corresponding thereto has its own MAD (Messages-Waiting Data) list, which stores the addresses Sc**1**, Sc**2** of those short message service centers SC which have attempted to transmit short messages to the subscriber basic service indicated by the MSISDN number (directory number), but the transmission has failed for some reason, for instance because the subscriber has not been reachable due to the fact that the terminal equipment of the subscriber has been located outside the coverage area of a radio network base station, i.e., in a shadow area, or due to the fact that the terminal equipment of the subscriber has been switched off.

FIG. **3** shows a subscriber MS connected to the cellular communication system via a base station BTS**1**, BTS**2**, base station controller BSC, and the mobile exchange VMSC/VLR of the location area of the subscriber. One or more short message service centers SC**1**, SC**2**, SC**3** store short messages to be transmitted to the subscriber MS. The short message service centers are connected to the cellular communication network via a gateway exchange GMSC/IWMSC. The visitor location register VLR of the location area of the subscriber stores information (Messages-Waiting-Flag) on the fact that a short message service center SC stores short messages to be transmitted to the subscriber. A subscriber location register **10**, which corresponds to a home location register HLR in the GSM system, contains an HLR function block **3**. The home location register of the invention also comprises a database in which information is maintained specific to the short message service center and to the subscriber, on the conditions on which the short message service center storing short messages of the subscriber is transmitted short message transmission starting messages. The database may be located in the subscriber database **11** as shown in FIG. **3**. The starting messages

(Alert) start the transmission of short messages from the short message service centers SC1, SC2, SC3 to the subscribers MS. When the subscriber MS has become reachable in the cellular communication network, the subscriber location register **10** obtains a notification thereof from the visitor location register VLR, because in the visitor location register there has been information, i.e., a set Messages-Waiting-Flag, on the fact that the short message service center SC contains short messages waiting to be transmitted to the subscriber MS. The HLR function block **3** of the subscriber location register thus requests information from the database **11** on the conditions on which the subscriber should be transmitted short messages, i.e., on what conditions the short message service center storing short messages intended for the subscriber should be transmitted said starting messages. It should be noted that the teleoperator controls the conditions included in said information maintained in the subscriber location register **10**; HLR so that the subscriber location register **10**; HLR transmits short message transmission starting messages (SMS Alert) to the short message service centers SC1, SC2, SC3 desired by the operator. After having made the request, the HLR function block **3** receives the conditions and decides based on the conditions if a short message transmission to the subscriber should be started. The effect of different conditions on a short message transmission will be described below. The HLR function block then controls according to the conditions the transmitter **1** transmits short message transmission starting messages, i.e., the starting message transmission functions, to transmit the short message starting messages of a certain subscriber, i.e., Alert messages in the case of a GSM network, to those short message service centers SC which have short messages to be transmitted to the subscriber MS and to which starting messages should be transmitted according to the conditions. The starting message transmitter **1** thus transmit short message starting messages so that the conditions which are maintained in the database and which are in accordance with the invention are observed. A short message service center SC1, first according to the conditions, included in the Messages-Waiting-Data-List of the subscriber location register **10**; HLR, associated with the IMSI, and corresponding to the subscriber's directory number, i.e., MSISDN number, is transmitted one short message transmission starting message, after which the starting message transmitter **1** waits for a predeterminable period before transmitting a second short message transmission starting message to the next short message service center SC2. In the GSM system, for instance, starting messages are transmitted so that the transmitter **1** requests the mobile applications part MAP communication protocol **2** located in the subscriber location register **10**; HLR to transmit a short message transmission starting message to the short message service center SC, whereby the MAP carries out the transmission of the starting message.

FIGS. **4–7** show a subscriber or subscriber station Mobile MS, the home location register HLR of said subscriber, and one or more short message service centers SC, which store short messages intended for the subscriber and which, according to the invention, transmit the short messages to the subscriber in accordance with predetermined conditions.

FIG. **4** shows a signaling diagram of a situation where the subscriber has become reachable, and only part of the short message transmission starting messages are transmitted. According to the invention, the subscriber location register HLR transmits short message transmission starting messages **404** to desired short message service centers in accordance with the conditions according to the invention. The transmission of the starting messages is started when the subscriber either transmits to her subscriber location register HLR a notification of the fact that the subscriber can be reached by the network again, i.e., a Note MS Present message **401**, performs a location updating, i.e., transmits an Update Location message **402**, or notifies the subscriber location register that the subscriber has memory capacity available by a Memory Capacity Available message **403**.

FIG. **5** shows a signaling diagram of a situation where a subscriber as become reachable, and short message transmission starting messages are transmitted to only certain short message service centers. The transmission of the starting messages is thus started by one of the above-mentioned messages **401–403** transmitted by the subscriber. The transmission of the starting messages can thus be prevented at the subscriber's request to all or part of the short message service centers. It is also possible that alerts destined for the addresses of only certain service centers are allowed. In FIG. **5**, this situation is illustrated by the fact that a starting message SMS Alert **505** is not going to another service center even if it goes to a desired service center.

FIG. **6** shows a signaling diagram of a situation where a subscriber has become reachable, and short message transmission starting messages are transmitted to only certain short message service centers, depending on the subscriber's location. In the situation shown in FIG. **6**, the transmission of starting messages is prevented based on the location of the receiving subscriber. This is based on the fact that the home location register HLR knows the location of the receiving subscriber MS with an accuracy of a mobile exchange, i.e., an MSC. Thus, a subscriber MS, for instance, which is located outside a certain area, for instance outside the service area of its own home mobile exchange, is not transmitted short messages, or short messages to be transmitted, located in a certain service center, are not transmitted to a certain subscriber. This characteristic can be used, for instance, when the subscriber is moving abroad and does not thus want to receive short messages from her home country. It is also possible to implement selective reception of short messages in such a manner that when moving abroad, the subscriber receives short messages only from the country she is located in. Naturally, it is also possible to implement other different and alternative solutions in selective short message reception.

FIG. **7** shows a signaling diagram of a situation where a subscriber requests and controls the transmission of short message transmission starting messages. In this embodiment, the subscriber, i.e., the mobile station or subscriber station, transmits to its subscriber location register HLR a control instruction, i.e., a Send SMS message **701**, by which the subscriber commands the subscriber location register to transmit desired short message transmission starting messages **705** to those short message service centers SC which have short messages to be transmitted to said subscriber MS. In this embodiment, the subscriber location register (home location register) HLR of the subscriber does not thus start transmitting starting messages after having received from the subscriber a Note MS Present message **401** or a location updating message Update Location or a notification of the fact that the subscriber has memory available, but starting messages are started to be transmitted only at the subscriber's specific request Send SMS.

The drawings and the description relating thereto are only intended to illustrate the idea of the invention. In their details, the method of the invention for starting a short message transmission in a cellular communication system, cellular communication system, and cellular communication

system subscriber location register may vary within the scope of the claims. Even if the invention has been described above mainly as applied in the GSM system, it can also be used in a radio system of a different type.

I claim:

1. A method for starting a short message transmission in a cellular communication network, comprising:

storing information in a subscriber location register based on the fact that at least one short message service center stores short messages to be transmitted to a subscriber to whom said short messages cannot be transmitted for the time being;

transmitting from said subscriber location register of said subscriber to said at least one short message service center, a short message transmission starting message when it is possible again to transmit short messages to said subscriber, wherein

information on conditions under which said short message service center is transmitted short message transmission starting messages is maintained specific to said short message service center and to said subscriber in said subscriber location register.

2. The method according to claim **1**, wherein said subscriber location register transmits said short message transmission starting messages concerning one subscriber to desired short message service centers, selectively, based on said maintained information so that starting messages are transmitted to only first short message service centers, which are desired to transmit short messages, and starting messages are not transmitted to second short message service centers, which are not desired to transmit short messages, even if said second short message service centers contain short messages to be transmitted to said subscriber.

3. The method according to claim **1**, wherein said subscriber controls said conditions included in said information maintained in said subscriber location register so that said subscriber location register transmits short message transmission starting messages to said short message service centers desired by said subscriber.

4. The method according to claim **3**, wherein in response to a control instruction transmitted by said subscriber, said subscriber location register does not transmit said starting messages.

5. The method according to claim **1**, wherein an operator controls said conditions included in said information maintained in said subscriber location register so that said subscriber location register transmits short message transmission starting messages to said short message service centers desired by said operator.

6. The method according to claim **1**, wherein said subscriber location register does not transmit said starting messages, if said subscriber is situated in a location other than a desired area.

7. The method according to claim **1**, wherein said subscriber location register transmits short message transmission starting messages to desired short message service centers in an order prioritized according to addresses of said short message service centers.

8. A cellular communication system, comprising

a subscriber;

at least one short message service center which transmits short messages to said subscriber via a cellular communication network and which stores short messages when the subscriber is not reachable; and

a subscriber location register of said subscriber, which contains information based on the fact that said at least one short message service center stores short messages to be transmitted to an unreachable subscriber, said subscriber location register comprising a transmitter which transmits a short message transmission starting message to said at least one short message service center when it is possible again to transmit short messages to said subscriber, wherein the subscriber location register comprises a database, maintaining information on conditions under which said short message service center is transmitted short message transmission starting messages specific to said short message service center and to said subscriber.

9. The cellular communication system according to claim **8**, wherein said subscriber location register further comprises a transmitter which transmits short message transmission starting messages to said short message service centers desired by said subscriber at the times desired by said subscriber.

10. A subscriber location register of a cellular communication system, comprising:

a transmitter which transmits a short message transmission starting message to at least one short message service center

a database, in which information on conditions under which said short message service center is transmitted short message transmission starting, messages is maintained specific to said short message service center and to said subscriber.

11. The subscriber location register according to claim **10**, further comprising:

a transmitter which transmits short message transmission starting messages to said short message service centers desired by said subscriber at times desired by said subscriber.

12. The subscriber location register according to claim **10**, further comprising:

a transmitter which transmits short message transmission starting messages to said short message service centers desired by said subscriber in an order prioritized according to said addresses of said short message service centers.

13. The subscriber location register according to claim **10**, further comprising:

an inhibitor which prevents transmission of short message transmission starting messages to said short message service centers desired by said subscriber, if said subscriber is situated in a location other than a desired area.

14. The subscriber location register according to claim **10**, wherein said subscriber location register is a GSM system home location register.

* * * * *

EXHIBIT C

US006112305A

United States Patent [19]

Dancs et al.

[11] Patent Number: 6,112,305

[45] Date of Patent: Aug. 29, 2000

[54] **MECHANISM FOR DYNAMICALLY BINDING A NETWORK COMPUTER CLIENT DEVICE TO AN APPROVED INTERNET SERVICE PROVIDER**

[75] Inventors: **Frank B. Dancs**, Hillsborough; **James E. Zmuda**, Foster City, both of Calif.

[73] Assignee: **Liberate Technologies**, San Carlos, Calif.

[21] Appl. No.: **09/073,271**

[22] Filed: **May 5, 1998**

[51] **Int. Cl.**[7] **H04L 9/00**

[52] **U.S. Cl.** **713/156**; 713/155; 713/161; 713/168; 380/255; 380/258

[58] **Field of Search** 380/255, 258; 713/161, 168, 170, 172, 173, 176, 156, 155

[56] **References Cited**

U.S. PATENT DOCUMENTS

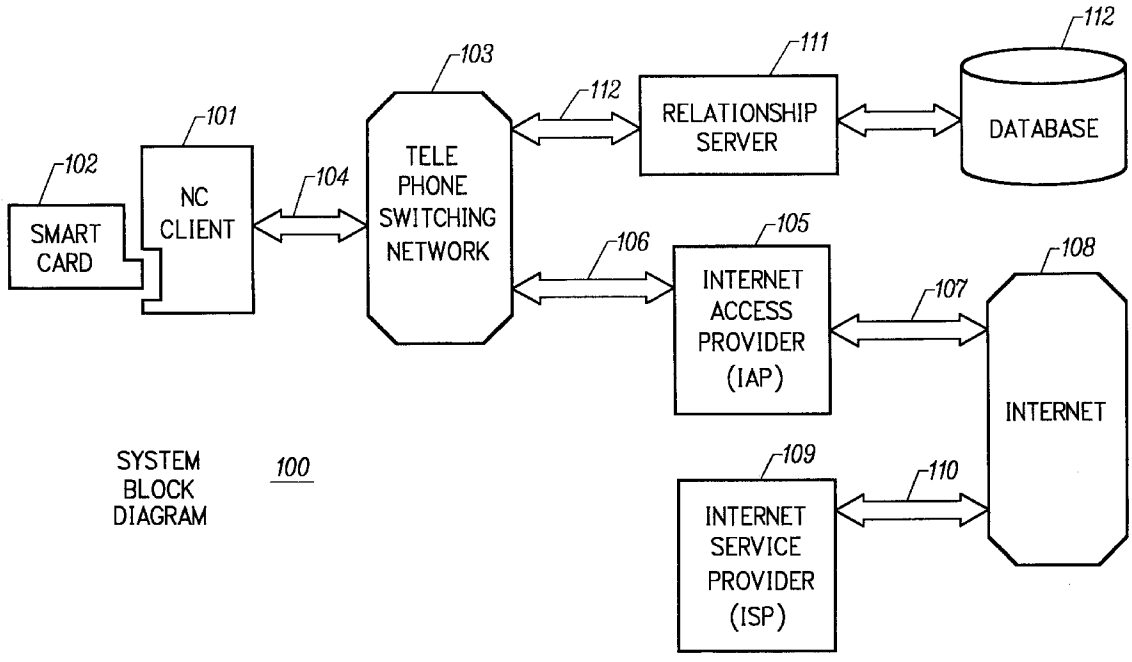
5,784,463	7/1998	Chen et al.	380/21
5,805,803	9/1998	Birrell et al.	395/187.01
5,857,024	1/1999	Nishino et al.	380/25
5,864,667	1/1999	Barkan	395/187.01
5,903,721	5/1999	Sixtus	395/187.01

Primary Examiner—Thomas R. Peeso
Attorney, Agent, or Firm—Fliesler, Dubb, Meyer & Lovejoy

[57] **ABSTRACT**

All network computer client device (NC) manufacturers' authorizations to connect to specific internet service providers (ISPs) are maintained in a central database associated with a relationship server. The relationship server issues digital certificates which associate various ISPs to their respective public keys. Each ISP is assigned a unique enterprise identification number by the relationship server. To authorize a specific ISP, the manufacturer begins with the relationship server's ISP certificate. The manufacturer computes and appends its own digital signature for the relationship server's ISP certificate, thereby creating an ISP usage certificate valid for its NCs which it sends back to the relationship server. Upon first powering on, each NC dials the relationship server and transmits its manufacturer identification number. The relationship server uses the manufacturer identification number to find the ISP usage certificates corresponding to the NC manufacturer. The relationship server then sends to the NC the ISP usage certificate corresponding to the enterprise identification number, or corresponding to the user's selection if no enterprise identification number on the smart card is established. The NC performs a cryptographic verification of the ISP usage certificate using the manufacturer's public key which is permanently stored in the NC in read only memory. Only if the verification of the ISP usage certificate is successful, thus indicating that the ISP usage certificate is signed by the manufacturer does the NC then attempts to connect to the ISP. When an ISP and manufacturer terminate an agreement, the relationship server disables the ISP's managed access software; when the NC's attempt to connect to the ISP fails, the NC then dials the relationship server to receive a new ISP usage certificate.

30 Claims, 15 Drawing Sheets



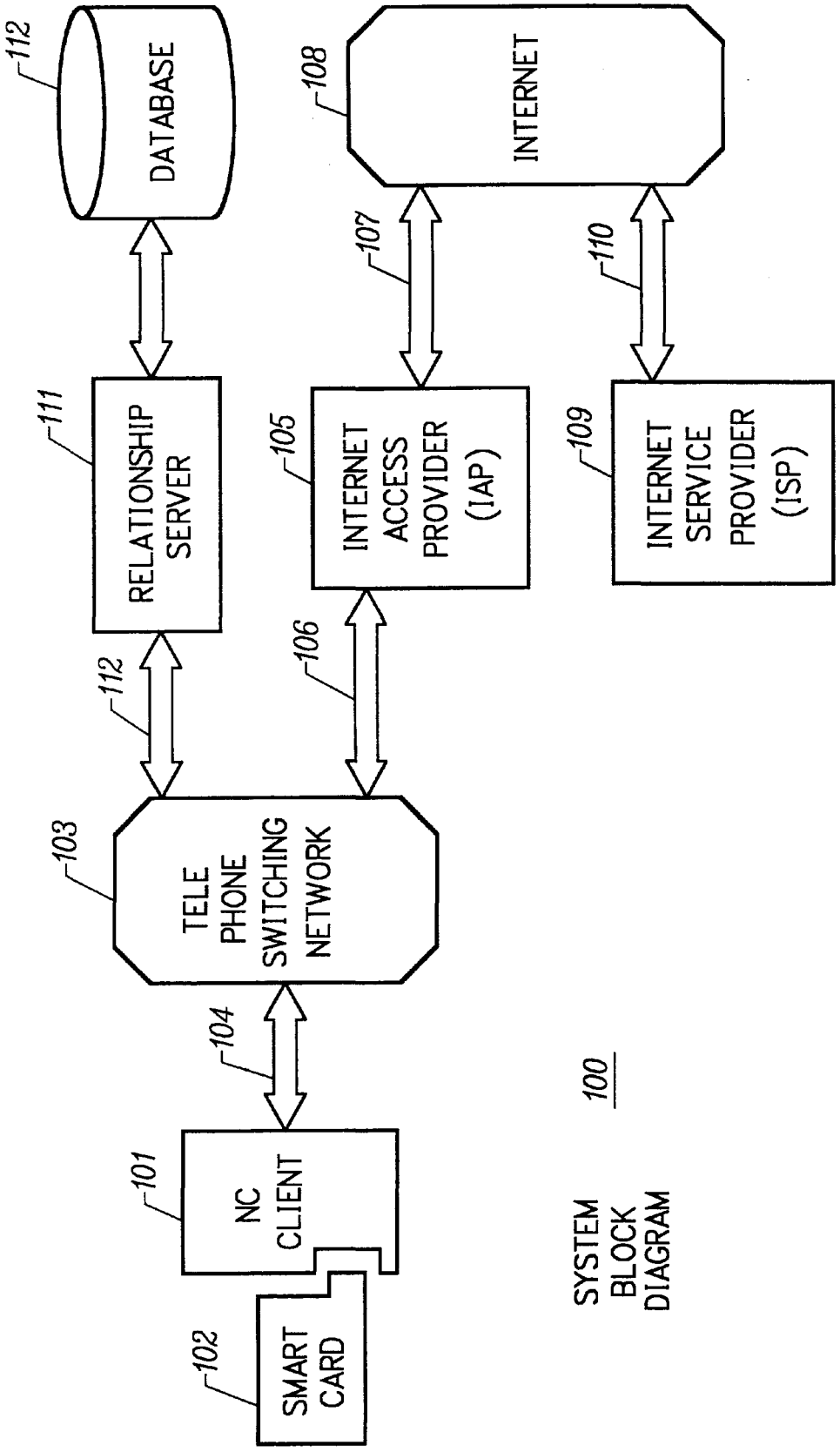
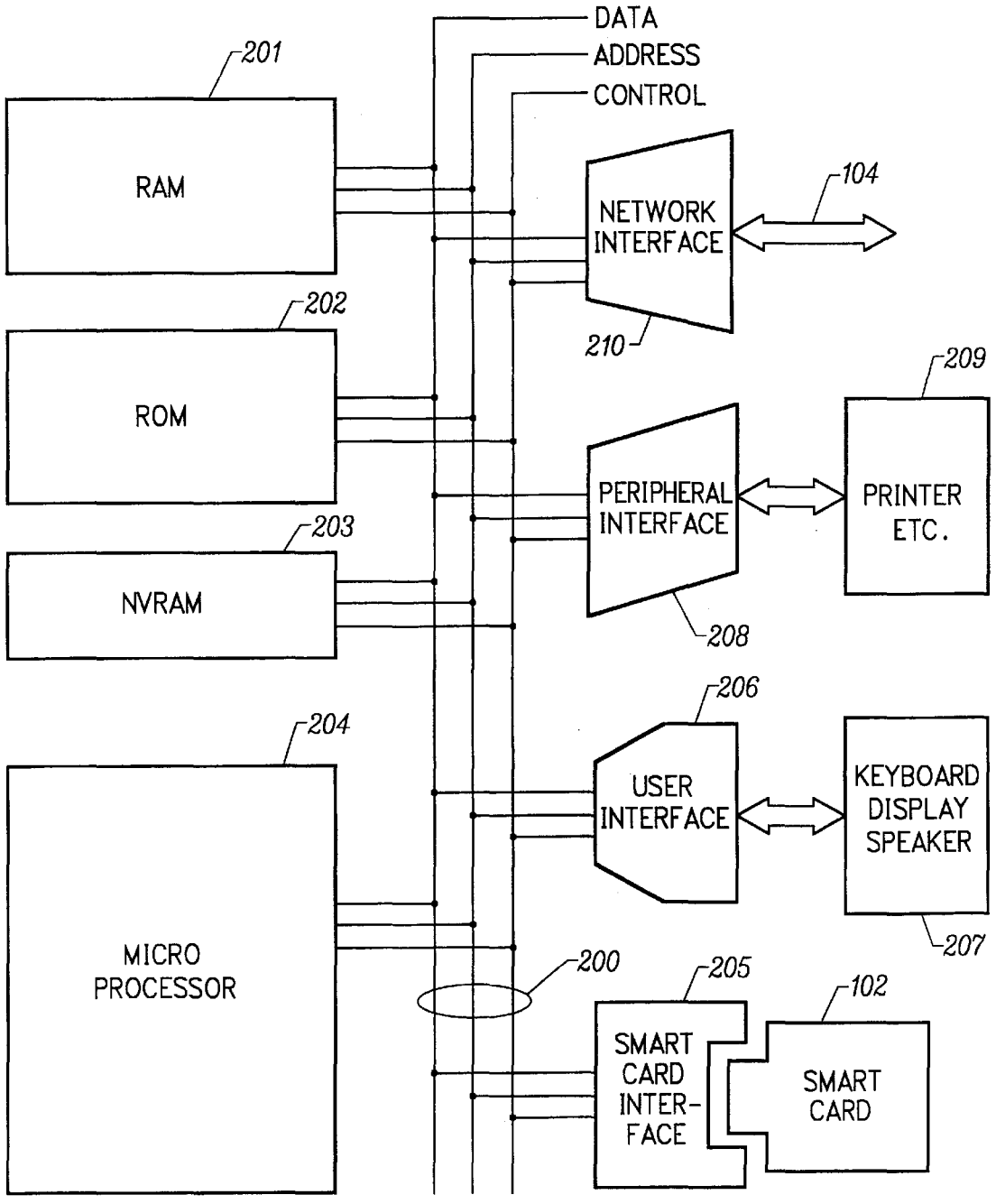

112
DATABASE
108
INTERNET
107
110
111
RELATIONSHIP SERVER
105
INTERNET ACCESS PROVIDER (IAP)
109
INTERNET SERVICE PROVIDER (ISP)
112
106
103
TELE PHONE SWITCHING NETWORK
104
101
NC CLIENT
102
SMART CARD
100
SYSTEM BLOCK DIAGRAM

FIG. 1



NC CLIENT BLOCK DIAGRAM 101

FIG. 2

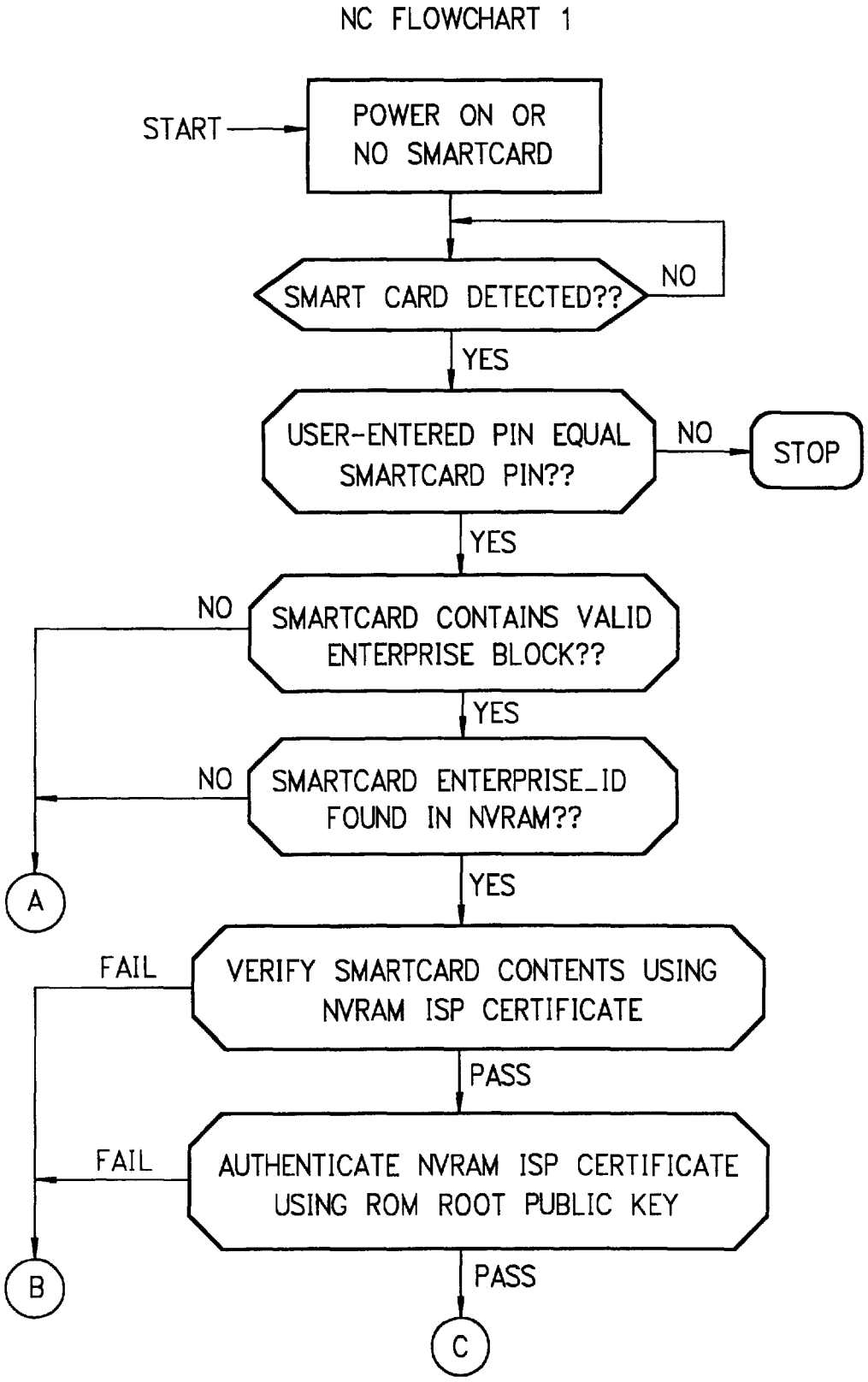

NC FLOWCHART 1
START
POWER ON OR NO SMARTCARD
SMART CARD DETECTED??
NO
YES
USER-ENTERED PIN EQUAL SMARTCARD PIN??
NO
STOP
YES
NO
SMARTCARD CONTAINS VALID ENTERPRISE BLOCK??
YES
NO
SMARTCARD ENTERPRISE_ID FOUND IN NVRAM??
YES
A
FAIL
VERIFY SMARTCARD CONTENTS USING NVRAM ISP CERTIFICATE
PASS
FAIL
AUTHENTICATE NVRAM ISP CERTIFICATE USING ROM ROOT PUBLIC KEY
B
PASS
C

FIG. 3

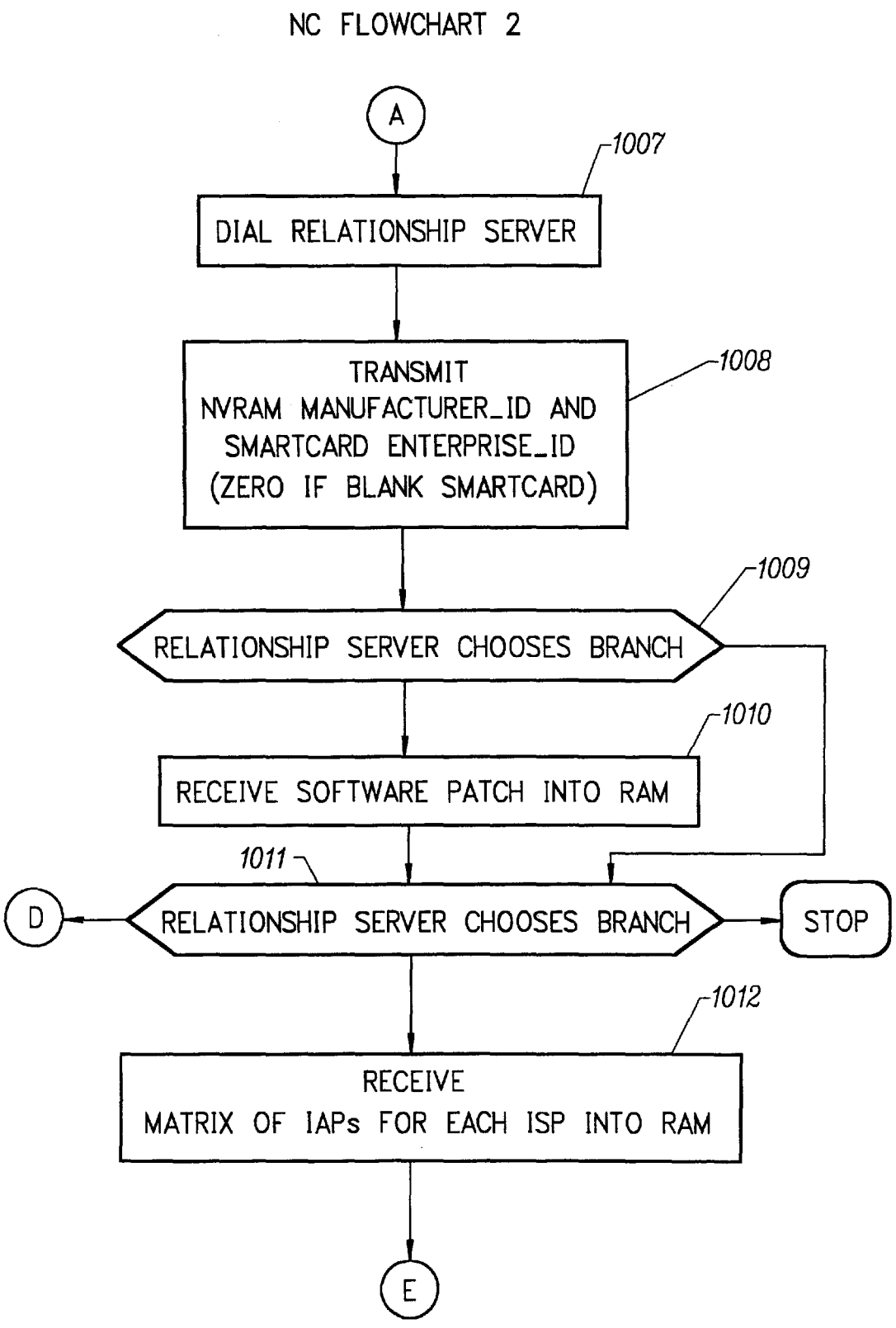

NC FLOWCHART 2
A
1007
DIAL RELATIONSHIP SERVER
TRANSMIT
NVRAM MANUFACTURER_ID AND
SMARTCARD ENTERPRISE_ID
(ZERO IF BLANK SMARTCARD)
1008
1009
RELATIONSHIP SERVER CHOOSES BRANCH
1010
RECEIVE SOFTWARE PATCH INTO RAM
1011
D
RELATIONSHIP SERVER CHOOSES BRANCH
STOP
1012
RECEIVE
MATRIX OF IAPs FOR EACH ISP INTO RAM
E

FIG. 4

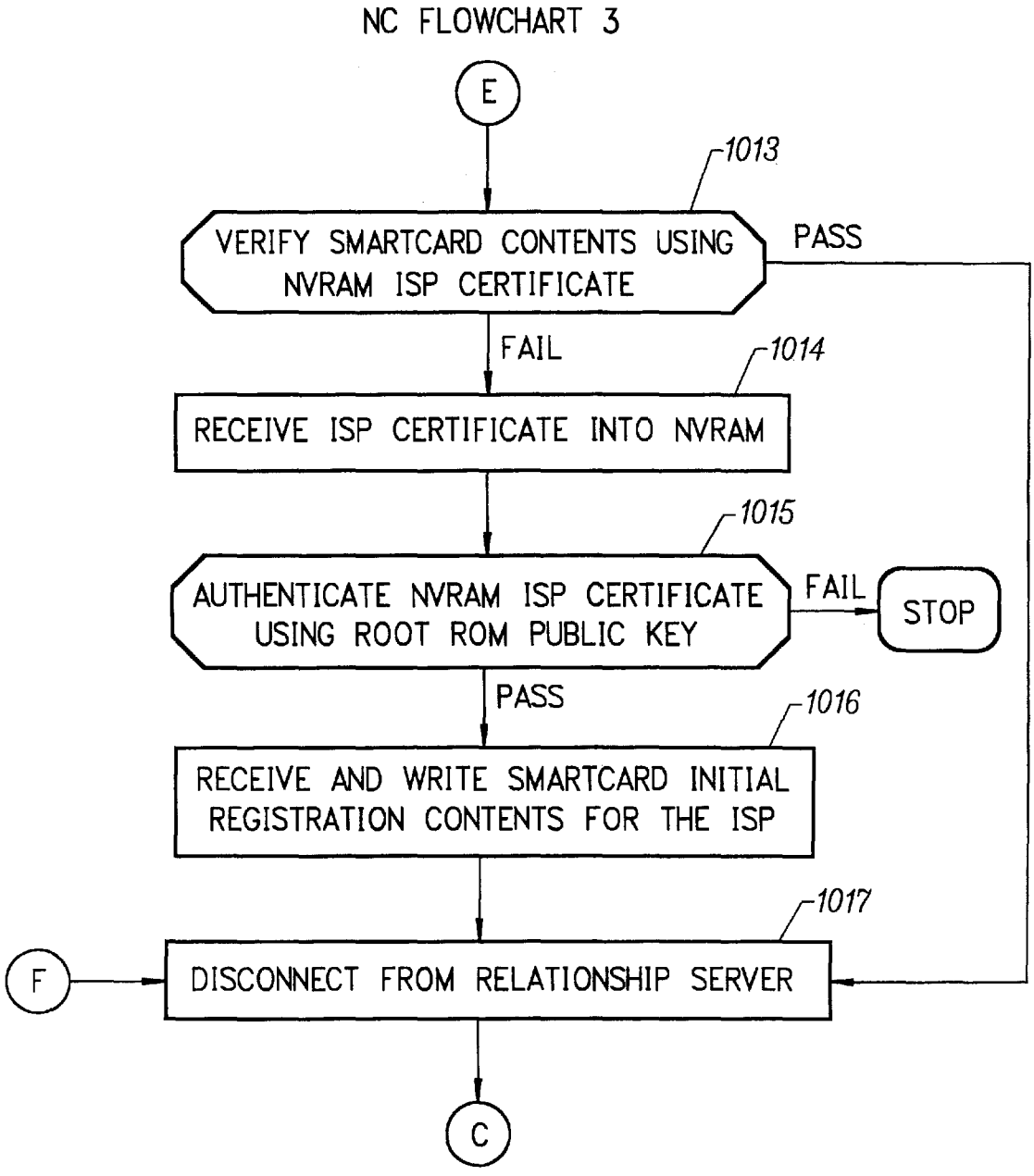

NC FLOWCHART 3
E
1013
VERIFY SMARTCARD CONTENTS USING NVRAM ISP CERTIFICATE
PASS
FAIL
1014
RECEIVE ISP CERTIFICATE INTO NVRAM
1015
AUTHENTICATE NVRAM ISP CERTIFICATE USING ROOT ROM PUBLIC KEY
FAIL
STOP
PASS
1016
RECEIVE AND WRITE SMARTCARD INITIAL REGISTRATION CONTENTS FOR THE ISP
1017
F
DISCONNECT FROM RELATIONSHIP SERVER
C

FIG. 5

NC FLOWCHART 4

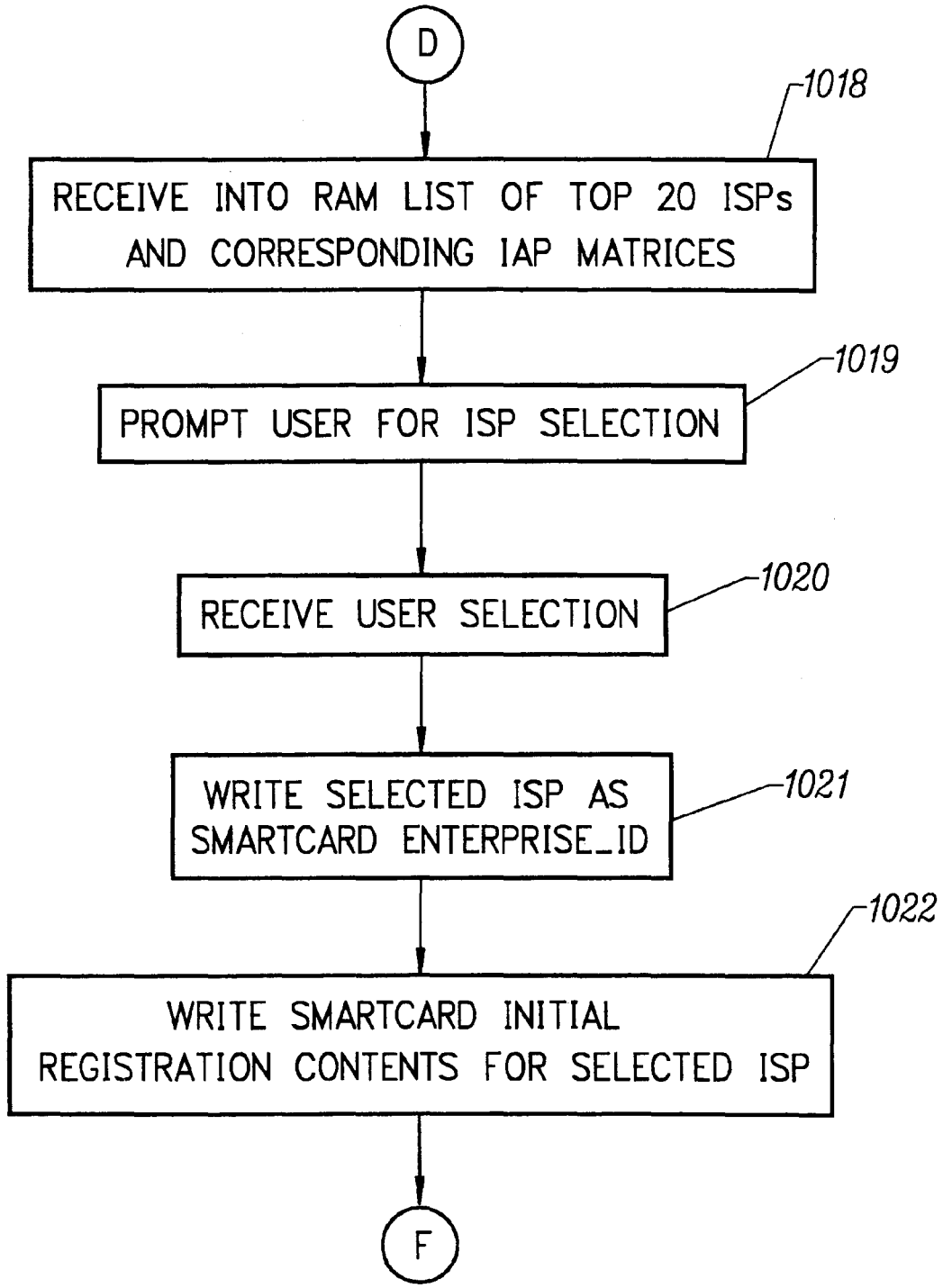


FIG. 6

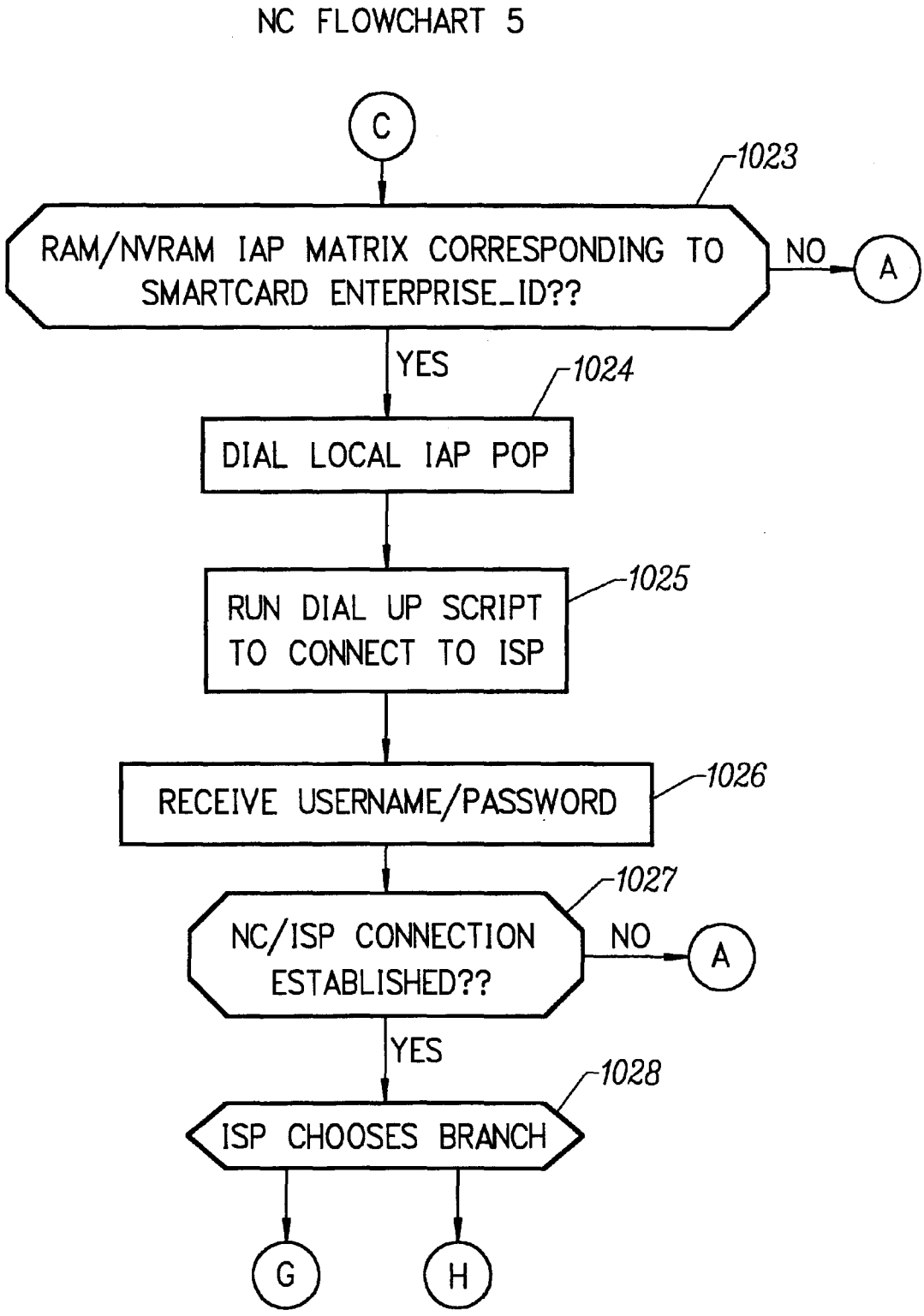

NC FLOWCHART 5
C
1023
RAM/NVRAM IAP MATRIX CORRESPONDING TO SMARTCARD ENTERPRISE_ID??
NO
A
YES
1024
DIAL LOCAL IAP POP
1025
RUN DIAL UP SCRIPT TO CONNECT TO ISP
1026
RECEIVE USERNAME/PASSWORD
1027
NC/ISP CONNECTION ESTABLISHED??
NO
A
YES
1028
ISP CHOOSES BRANCH
G
H

FIG. 7

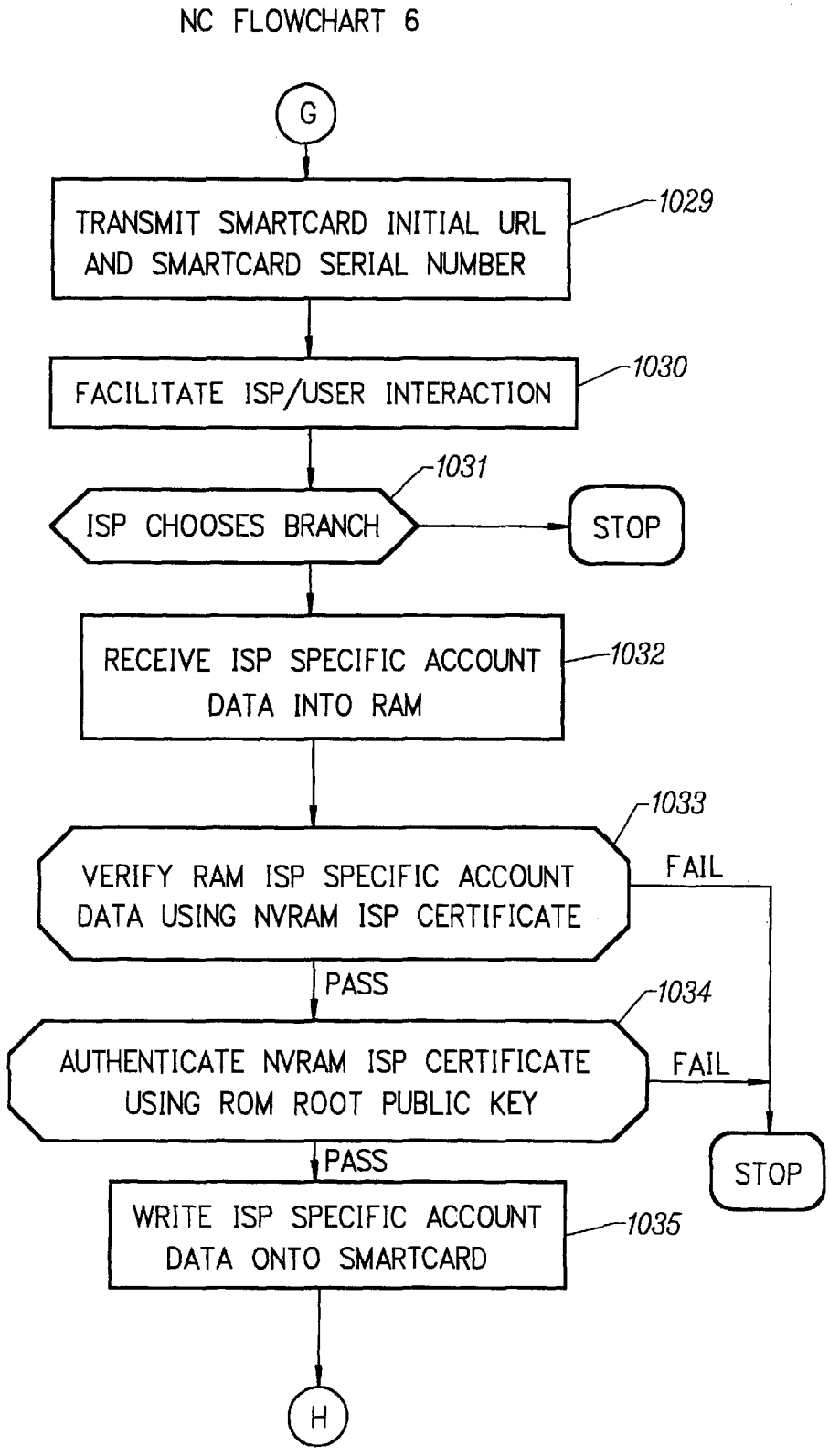

NC FLOWCHART 6
G
TRANSMIT SMARTCARD INITIAL URL AND SMARTCARD SERIAL NUMBER
1029
FACILITATE ISP/USER INTERACTION
1030
ISP CHOOSES BRANCH
1031
STOP
RECEIVE ISP SPECIFIC ACCOUNT DATA INTO RAM
1032
VERIFY RAM ISP SPECIFIC ACCOUNT DATA USING NVRAM ISP CERTIFICATE
1033
FAIL
PASS
AUTHENTICATE NVRAM ISP CERTIFICATE USING ROM ROOT PUBLIC KEY
1034
FAIL
STOP
PASS
WRITE ISP SPECIFIC ACCOUNT DATA ONTO SMARTCARD
1035
H

FIG. 8

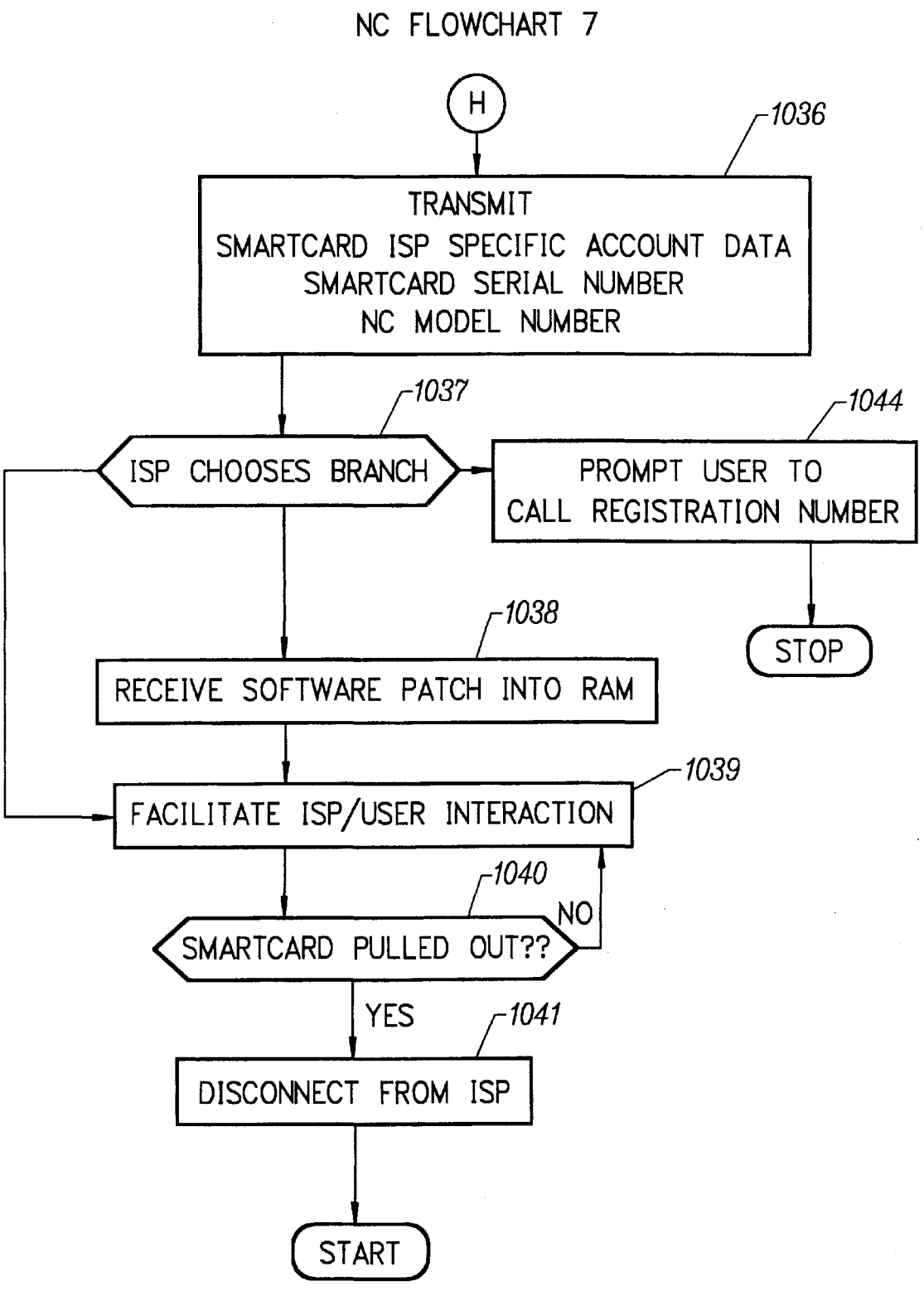

NC FLOWCHART 7
H
1036
TRANSMIT
SMARTCARD ISP SPECIFIC ACCOUNT DATA
SMARTCARD SERIAL NUMBER
NC MODEL NUMBER
1037
ISP CHOOSES BRANCH
1044
PROMPT USER TO
CALL REGISTRATION NUMBER
STOP
1038
RECEIVE SOFTWARE PATCH INTO RAM
1039
FACILITATE ISP/USER INTERACTION
1040
NO
SMARTCARD PULLED OUT??
YES
1041
DISCONNECT FROM ISP
START

FIG. 9

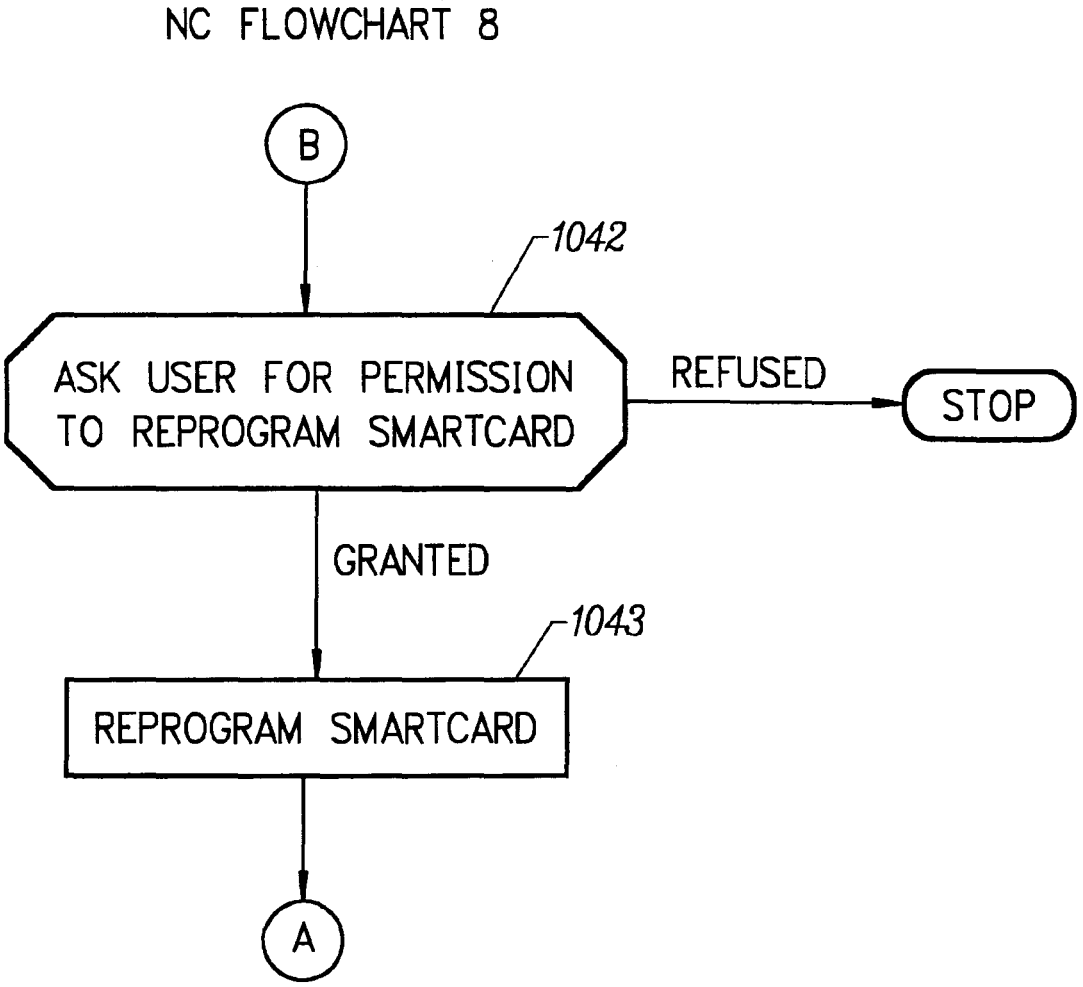

NC FLOWCHART 8
B
1042
ASK USER FOR PERMISSION TO REPROGRAM SMARTCARD
REFUSED
STOP
GRANTED
1043
REPROGRAM SMARTCARD
A

FIG. 10

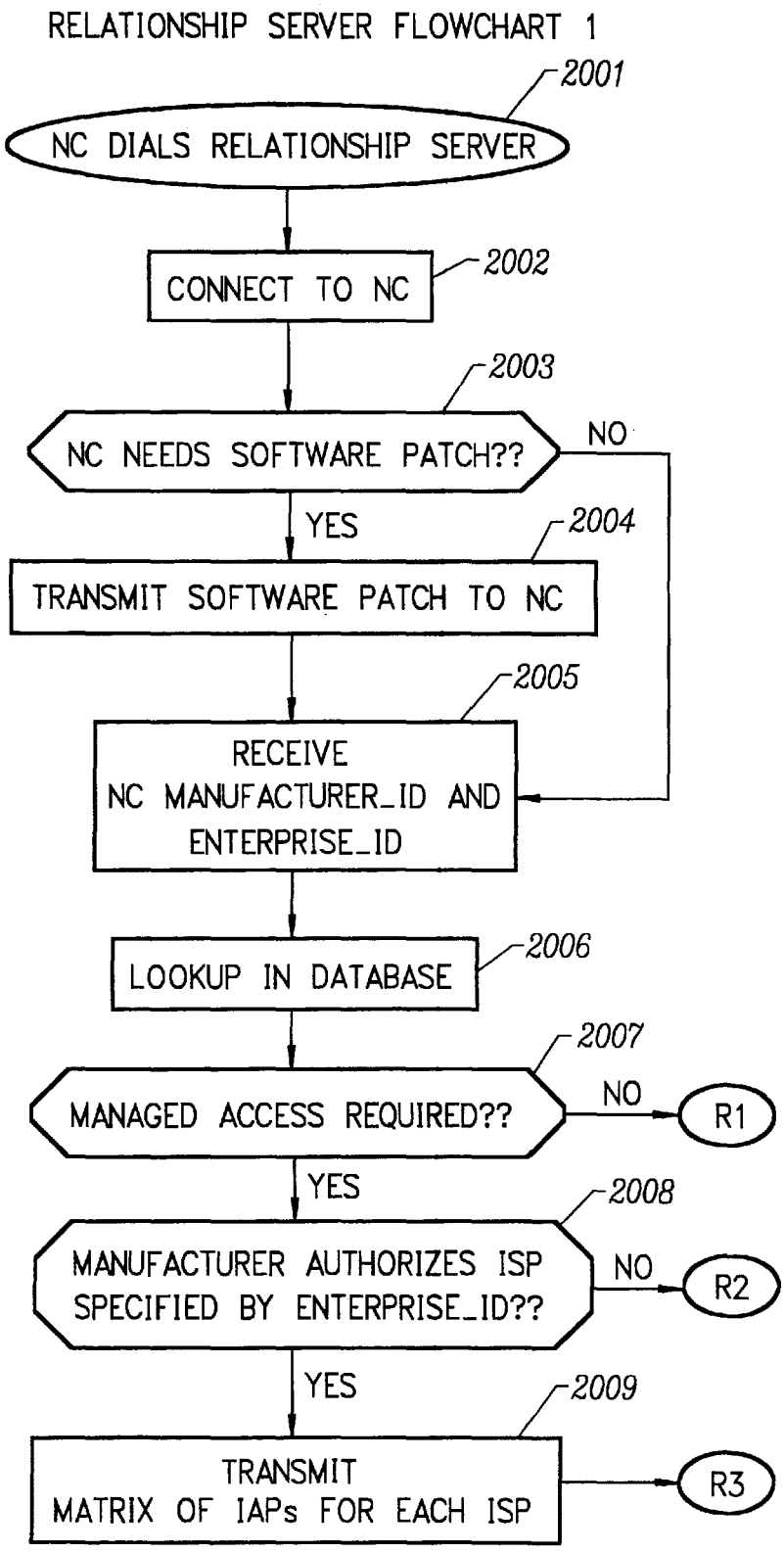

RELATIONSHIP SERVER FLOWCHART 1
2001
NC DIALS RELATIONSHIP SERVER
CONNECT TO NC
2002
2003
NC NEEDS SOFTWARE PATCH??
NO
YES
2004
TRANSMIT SOFTWARE PATCH TO NC
2005
RECEIVE
NC MANUFACTURER_ID AND
ENTERPRISE_ID
LOOKUP IN DATABASE
2006
2007
MANAGED ACCESS REQUIRED??
NO
R1
YES
2008
MANUFACTURER AUTHORIZES ISP
SPECIFIED BY ENTERPRISE_ID??
NO
R2
YES
2009
TRANSMIT
MATRIX OF IAPs FOR EACH ISP
R3

FIG. 11

RELATIONSHIP SERVER FLOWCHART 2

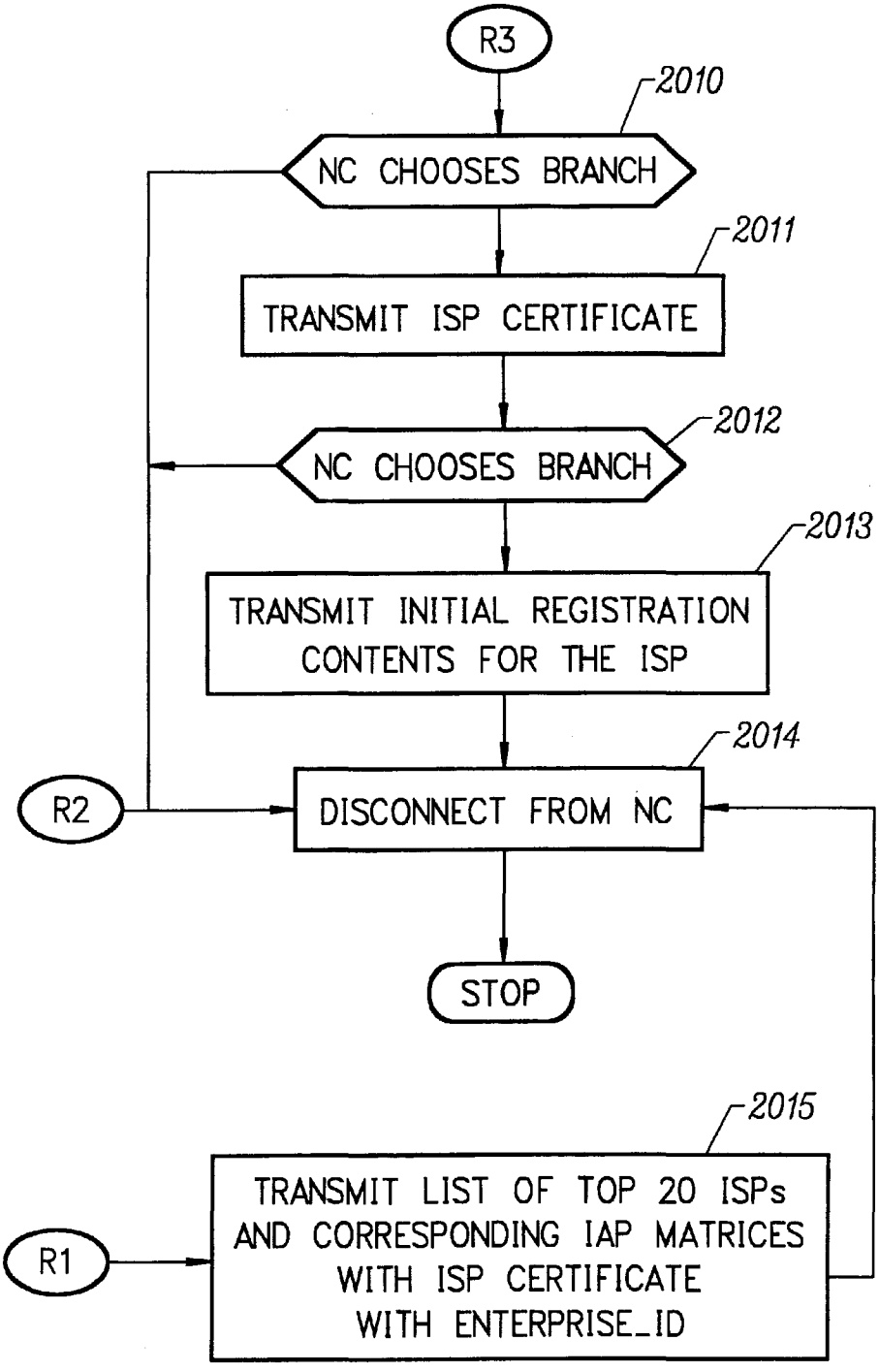


FIG. 12

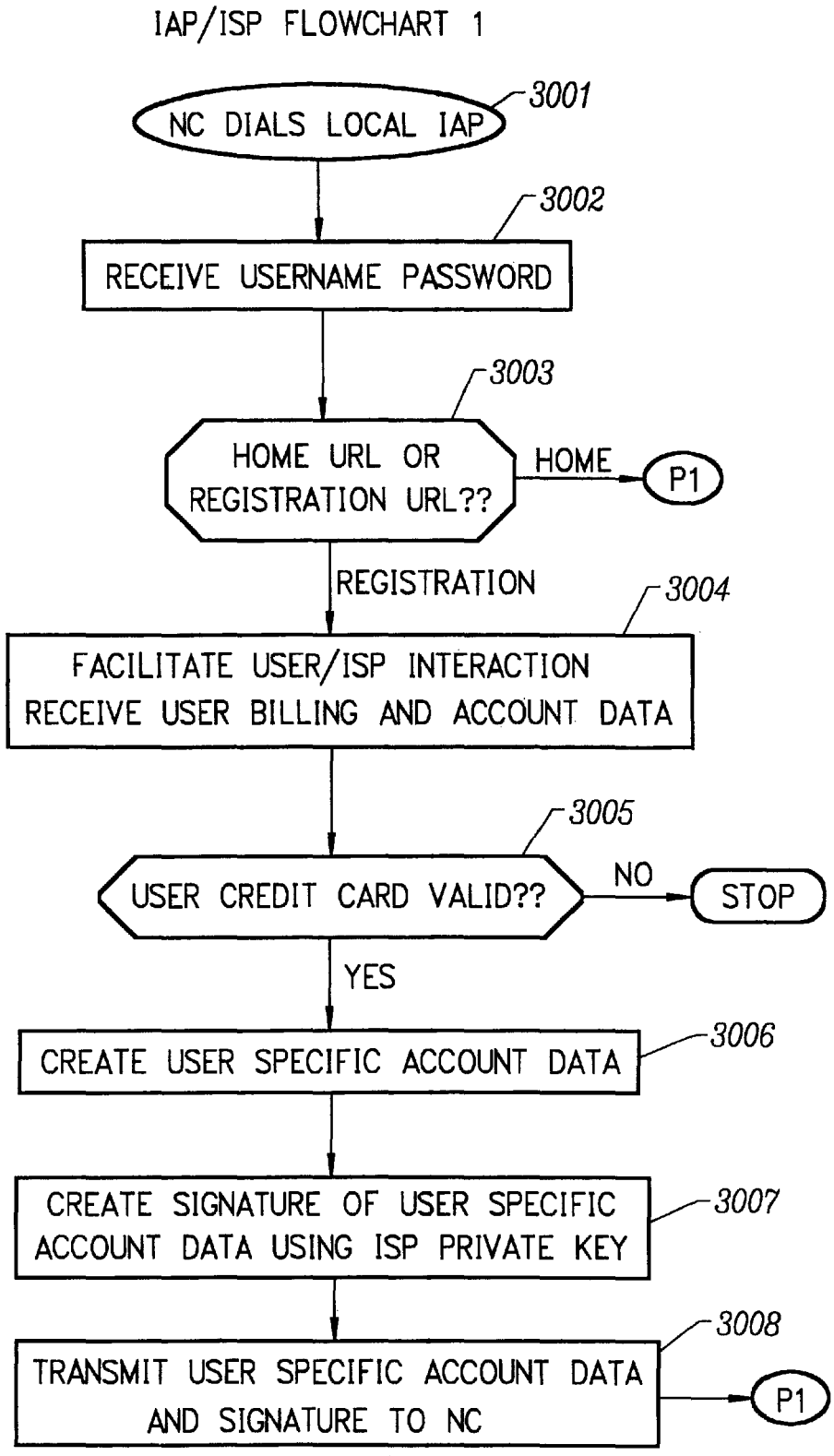

IAP/ISP FLOWCHART 1
NC DIALS LOCAL IAP
3001
RECEIVE USERNAME PASSWORD
3002
HOME URL OR REGISTRATION URL??
3003
HOME
P1
REGISTRATION
FACILITATE USER/ISP INTERACTION
RECEIVE USER BILLING AND ACCOUNT DATA
3004
USER CREDIT CARD VALID??
3005
NO
STOP
YES
CREATE USER SPECIFIC ACCOUNT DATA
3006
CREATE SIGNATURE OF USER SPECIFIC ACCOUNT DATA USING ISP PRIVATE KEY
3007
TRANSMIT USER SPECIFIC ACCOUNT DATA AND SIGNATURE TO NC
3008
P1

FIG. 13

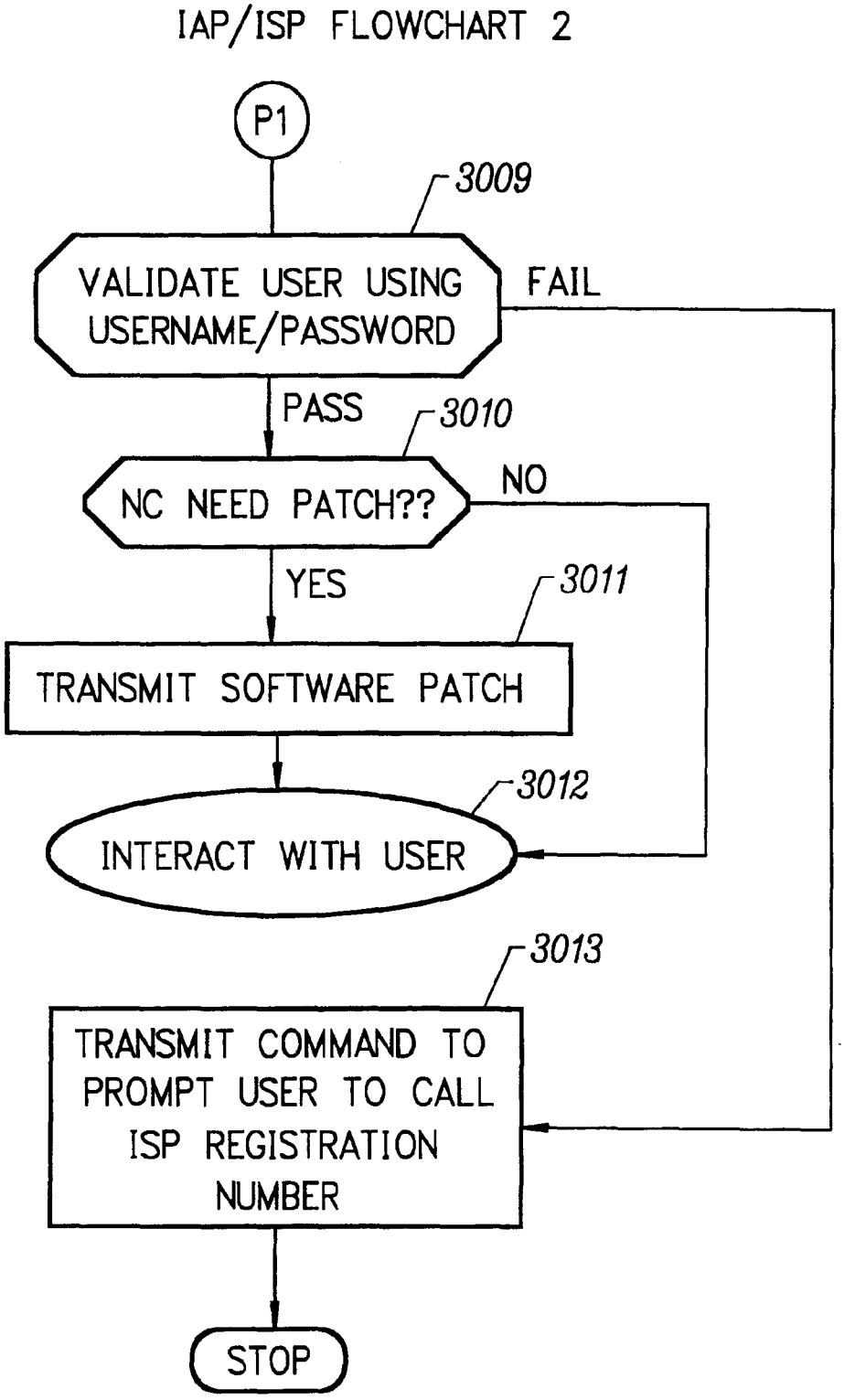

IAP/ISP FLOWCHART 2
P1
3009
VALIDATE USER USING USERNAME/PASSWORD
FAIL
PASS
3010
NC NEED PATCH??
NO
YES
3011
TRANSMIT SOFTWARE PATCH
3012
INTERACT WITH USER
3013
TRANSMIT COMMAND TO PROMPT USER TO CALL ISP REGISTRATION NUMBER
STOP

FIG. 14

1501

NVRAM	
RELATIONSHIP SERVER TELEPHONE NUMBER	M
MANUFACTURER SERIAL NUMBER	M
ENTERPRISE_ID	RS
ISP CERTIFICATE	RS
IAP MATRIX FOR ENTERPRISE_ID	RS
IAP_ID	RS
DNS1	RS
DNS2	RS
DIAL SCRIPT	RS
IAP RULES	RS
POP TELEPHONE NUMBER	RS

1502

RAM	
ALL AVAILABLE ENTERPRISE_IDs	RS
IAP MATRIX FOR EACH ENTERPRISE_ID	RS

1503

ROM	
RELATIONSHIP SERVER PHONE NUMBER	*
ROOT AUTHORITY PUBLIC KEY	*

1504

SMARTCARD ISP BLOCK	
ENTERPRISE_ID	RS, *
URL	RS, ISP
R/W MOUNT POINT	RS, ISP
NFS/CSFS FILE SERVER	RS, ISP
ISP SIGNATURE	RS, ISP
PROXY SERVER	RS, ISP

FIG. 15

MECHANISM FOR DYNAMICALLY BINDING A NETWORK COMPUTER CLIENT DEVICE TO AN APPROVED INTERNET SERVICE PROVIDER

CROSS-REFERENCE TO RELATED APPLICATIONS

This Application is related to the following Applications:

(1) "Mechanism for Users with Internet Service Provider Smart Cards to Roam Among Geographically Disparate Authorized Network Computer Client Devices Without Mediation of a Central Authority," by Frank B. Dancs and James E. Zmuda.

(2) "Mechanism for Facilitating Secure Storage and Retrieval of Information on a Smart Card by an Internet Service Provider Using Various Network Computer Client Devices," by Frank B. Dancs and James E. Zmuda.

(3) "Internet Service Provider Preliminary User Registration Mechanism Provided by Centralized Authority," by Frank B. Dancs and James E. Zmuda.

Each of these related Applications is incorporated herein by reference.

BACKGROUND OF THE INVENTION

1. Field of the Invention

The present invention is in the field of network computer client devices (NCs) which rely upon a network connection to supply all necessary program files and data files. The present invention operates in an environment in which a relationship server is a central contact point for all NCs. Specifically, the present invention addresses the desire of NC manufacturers to authorize usage of their NCs only to connect to certain specific internet service providers (ISPs).

2. Discussion of the Related Art

In a network-centric computing environment, the three major computing components are a network computer client device (NC), a server device, and a smart card. The NC does not contain a hard disk, and therefore relies upon a network connection for virtually all program and data. Therefore, the NC needs the server device for booting security, file storage, and system management. The smart card is used to identify and authenticate a particular user and to carry individual information about the user. The user combines his smart card with an NC to access his logical workspace from the NC.

In the network-centric computing environment, there are several business entities. An internet service provider (ISP) is the entity with which the user has an agreement to provide basic server resources. An internet access provider (IAP) is an entity with which the ISP has a relationship for provision of its internet protocol (IP) address to enable users to connect to the internet. An ISP may function as its own IAP. An NC client device manufacturer builds NCs.

The various NC client device manufacturer desire the ability to control the ISPs to which their NCs can connect.

SUMMARY OF THE INVENTION

A network computer client device (NC) manufacturer desires the ability to authorize usage of its NCs only to access those specific internet service providers (ISPs) with which it has established business relationships. These authorizations may change over time and the NC manufacturer desires the ability to change the ISP connection capabilities of its NCs so as to facilitate connection only to those currently authorized ISPs.

According to an aspect of the present invention, all manufacturers' authorizations to connect to specific ISPs are maintained in a central database associated with a relationship server. The manufacturers may change these authorizations over time. The relationship server issues digital certificates, such as X.509 certificates in the preferred embodiment, which associate various ISPs to their respective public keys. Each ISP is assigned a unique number by the relationship server. In the preferred embodiment, the serial number associated with each certificate becomes an enterprise identification number which uniquely identifies the ISP designated in the certificate. To authorize a specific ISP, the manufacturer begins with the relationship server's ISP certificate. Using its own private key, the manufacturer computes its own digital signature for the relationship server's ISP certificate and appends this digital signature to the relationship server's ISP certificate, thereby creating an ISP usage certificate valid for its NCs. After digitally signing all the relationship server's ISP certificates for which the manufacturer desires to authorize connection to its NCs, the manufacturer delivers all its ISP usage certificates back to the relationship server. The manufacturer may send additional ISP usage certificates to the relationship server at any time, and may revoke existing ISP usage certificates.

According to another aspect of the present invention, upon first powering on, each NC dials the relationship server and transmits its manufacturer identification number. The relationship server uses the manufacturer identification number to find the ISP usage certificates corresponding to the NC manufacturer. In the preferred embodiment, the NC also sends the relationship server an enterprise identification number from the user's smart card. The relationship server then sends to the NC the ISP usage certificate corresponding to the enterprise identification number, or corresponding to the user's selection if no enterprise identification number on the smart card is established.

According to another aspect of the present invention, the NC performs a cryptographic verification of the ISP usage certificate using the manufacturer's public key which is permanently stored in the NC in read only memory, for example. Only if the verification of the ISP usage certificate is successful, thus indicating that the ISP usage certificate is signed by the manufacturer does the NC then attempts to connect to the ISP.

According to yet another aspect of the present invention, ISP managed access software controlled by the relationship server is required to interface an NC to an ISP. When an ISP and manufacturer terminate an agreement, the relationship server disables the ISP's managed access software. A stale ISP usage certificate may exist on an NC if an ISP authorization has been revoked by the manufacturer since the NC's last connection to the relationship server. In this event according to the present invention, when the NC's attempt to connect to the ISP fails because of the disabled ISP managed access software, the NC then dials the relationship server to receive a new ISP usage certificate corresponding to a different, and perhaps newly authorized ISP.

In the preferred embodiment of the present invention, the ISP usage certificates, the relationship server telephone number, and the manufacturer serial number are stored in a non-volatile memory within the NC, and the manufacturer's public key is stored in a read only memory.

These and other features and advantages of the present invention will be apparent from the Detailed Description of the Invention in conjunction with the Figures

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1 illustrates the distributed computing system architecture in accordance with the present invention.

FIG. **2** is a block diagram illustrating the logical architecture of a network computer client device (NC) in accordance with the present invention.

FIG. **3** is the first flow chart illustrating the method of operation of the NC in accordance with the present invention.

FIG. **4** is the second first flow chart illustrating the method of operation of the NC in accordance with the present invention.

FIG. **5** is the third flow chart illustrating the method of operation of the NC in accordance with the present invention.

FIG. **6** is the fourth flow chart illustrating the method of operation of the NC in accordance with the present invention.

FIG. **7** is the fifth flow chart illustrating the method of operation of the NC in accordance with the present invention.

FIG. **8** is the sixth flow chart illustrating the method of operation of the NC in accordance with the present invention.

FIG. **9** is the seventh flow chart illustrating the method of operation of the NC in accordance with the present invention.

FIG. **10** is the eighth flow chart illustrating the method of operation of the NC in accordance with the present invention.

FIG. **11** is the first flow chart illustrating the method of operation of the relationship server in accordance with the present invention.

FIG. **12** is the second flow chart illustrating the method of operation of the relationship server in accordance with the present invention.

FIG. **13** is the first flow chart illustrating the method of operation of the internet access provider (IAP) and internet service provider (ISP) in accordance with the present invention.

FIG. **14** is the second flow chart illustrating the method of operation of the IAP and ISP in accordance with the present invention.

FIG. **15** illustrates the various fields of the non-volatile memory (NVRAM), random access memory (RAM), and read only memory (ROM) within the NC and the contents of the smart card, as well as indicating who has permission to write the various fields, in accordance with the present invention.

In the FIGS. **1** through **15**, like parts are referred to with like reference numerals. The Figures. are more thoroughly explained in the Detailed Description of the Invention.

DETAILED DESCRIPTION OF THE INVENTION

The present invention operates in the environment of a system for providing managed access to network computer devices (NCs). NC manufacturers and distributers may utilize the methods of the present invention to ensure that the NCs they manufacturer or distribute are able to connect only to internet service providers (ISPs) that they authorize. Some manufacturers and distributors may provide their own internet service; other manufacturers or distributors will contract with ISP partners to provide internet service for the NCs they manufacture or distribute. NCs accept and require smart cards to be inserted before becoming operational to connect to an ISP. Each smart card is typically associated with an individual user. A smart card ultimately will contain information pertinent to a specific user's relationship with one or more specific ISPs.

According to the managed access environment, a specific NC will only provide internet service connectivity when a smart card is inserted that has been at least preliminarily registered with a partner ISP of the NCs manufacturer or distributor.

FIG. **1** illustrates the key components of the managed access environment **100** according to the present invention. An NC client **101** accepts a smart card **102**. The NC client **101** communicates through the telephone system **103** using a standard telephone line **104**, such as POTS (plain old telephone service) or ISDN (integrated services digital network). An internet access provider (IAP) **105** is also connected to the telephone system **103**, and can be reached by dialing its telephone number. The IAP **105** contains a modem bank (not shown) which receives data from its telephone line **106** and transmits the data in the appropriate internet format on its internet connection **107** onto the internet **108**.

An ISP **109** also has a digital link **110** to the internet **108** which allows it to receive data sent from the NC client **101** through the IAP **105**. The ISP **109** also sends data to the NC client **101** through the IAP **105** modem bank (not shown). A relationship server **111** is also connected to the telephone switching network **103** through a standard telephone line and can be reached by dialing a specific toll free number such as 1-800-735-2846, which corresponds to 1-800-RELATIONSHIP. The relationship server **111** is connected to a database **112** which maintains information regarding manufacturer or distributer relationships with ISPs.

According to present invention, the smart card **102** may be written with an alternative relationship server telephone number to be used in the event that relationship server **111** hard coded into the ROM **202** is stopped or a relationship between the manufacturer and the relationship server **111** is terminated. The alternative relationship server telephone number is signed by the entity owning the root public key found in the ROM **202**.

An IAP **105** (Internet Access Provider) is the corporate entity providing Internet Protocol (IP) Addresses and other boot services; perhaps distinct from the Telecommunications company providing communication hardware. An ISP (Internet Service Provider) is the corporate entity the NC User has an agreement with to provide content (e.g. NetChannel, AOL, CompuServe). An NC User is an individual in possession of an NC smart card **102**. An ENTERPRISE_ID is a unique identifier for either an ISP **109** or corporate client.

FIG. **2** is a block diagram showing a possible configuration of an NC client **101** suitable for use in the managed access system according to the present invention. The NC **101** includes a random access memory (RAM) **201**, a read only memory (ROM) **202**, and non-volatile random access memory (NVRAM) **203** which are all tied to a microprocessor **204** via an internal bus **200**. The smart card **102** connects to a smart card interface unit **205** which also connects to the internal bus **200**. A user interface **206** provides interfaces the internal bus **200** to all the user interface apparatus **207**. Thus, the user interface **206** accepts inputs from a keyboard and drives a display and speaker. A peripheral interface **208** connects the internal bus **200** to any possible peripherals **209**, such as a printer or facsimile machine. A network interface **210** connects the internal bus **200** to the telephone network **103** through the telephone line

104. The block diagram illustrated in FIG. 2 for the NC client 101 is shown by way of example, not by way of limitation. For example, the NVRAM 203 is entirely optional, RAM 201 can alternatively be used to provide the functions as described herein in the context of the preferred embodiment as being provided by the NVRAM 203. A wide variety of general purpose computing devices can be constructed to operated as NCs so long as they include sufficient RAM 201, ROM 202, and NVRAM 203 and can accommodate a smart card 102 and network connection 104. Furthermore, the internal organization of the NC client 101 is not limited to the single bus 200 architecture shown in FIG. 2. For example, the RAM 201, ROM 202, and NVRAM 203 might be tied to the microprocessor 204 using a memory bus 200, while the smart card interface 205, user interface 206, peripheral interface 208 (if present), and network interface 210 are tied to the microprocessor using one or more separate internal busses (not shown). NVRAM 203 is optional; the RAM 201 can be used in the alternative to NVRAM 203 to provide the same functions. In addition, other elements can be added to the NC client 101. For example, a separate system controller chip (not shown) or graphics or cryptographic accelerator (not shown) may also be included in the NC client 101.

The NC client 101 typically does not include a hard disk drive. Therefore, aside from the small amount of boot code and other data stored in the ROM 202, all code and data which the NC client 101 uses is provided to it through its network connection 104. According to the present invention, managed access requires that a manufacturer's NCs are tied to the manufacturer's partner ISP 109. Because the NC client 101 does not have a hard disk drive, the NC client 101 is essentially useless without the manufacturer's partner ISP 109.

According to the managed access system of the present invention, a specific manufacturer's NC client 101 can only be used with authorized services; conversely, the NC client 101 is prevented from accessing unauthorized services according to the present invention. The NC client 101 is required to connect to the relationship server 111 upon its first use when its NVRAM 203 is empty. The relationship server 111 maintains a database 112 including all manufacturers' unique identification numbers and the relationships those manufacturers have with various ISPs. When the NC client 101 is first switched on it calls the relationship server 111 and transmits its unique device identification number. Its device identification number is a composite which includes the manufacturer identification number, the model number, and the device serial number. The relationship server 111 looks up the manufacturer identification number in the database 112, finds the manufacturer, and then scans the list of partner ISPs. If the relationship server 111 finds a suitable ISP partner in the database 112, the relationship server 111 sends back to the NC client 101 connect information for the partner ISP services, and for the various IAPs which correspond to the partner ISP services. In the event that the relationship server 111 is run by an ISP 109, then the database 112 contains information regarding which manufacturers have a relationship with the ISP 109.

According to the managed access system of the present invention, users of authorized services may roam to various NC clients which are made by the same manufacturer. Additionally, users may roam to various NC clients manufactured by different manufacturers so long as the different NC manufacturers each authorize connection to the roaming user's ISP service.

User roaming to various NC client devices made by the same manufacturer occurs when a user of NC client A made by manufacturer A to connect to an ISP moves to NC client B made by manufacturer A and inserts his personal smart card 102 to connect to the ISP. In this event, the NC client B reads the ENTERPRISE_ID on the smart card 102 to determine if the ENTERPRISE_ID matches anything the NC client B has in its RAM 201. If a match exists, then a check of NVRAM 203 is performed for a valid account with a valid IAP 105 to get to the ISP. If the NC client B locates a match in NVRAM 203, then the NC client B will dial the local IAP 105 and will allow the user to login into the ISP 109. The ISP 109 holds 'home' server information for the user and is therefore able to grant access to the user's files from wherever the user is. If the NC client B does not contain the ENTERPRISE_ID found on the user's smart card 102, then the NC client B will call the relationship server 111 to find out if there has been a new agreement established by the NC client manufacturer since its last call to the relationship server 111. If the manufacturer has indeed established a new partner identified by the user's ENTERPRISE_ID, the NC client 101 downloads the new ISP and corresponding IAP information and connects to the new ISP identified by the user's ENTERPRISE_ID.

User roaming to NC client devices made by different manufactures occurs when a user of NC client A made by manufacturer A to connect to an ISP moves to NC client B made by manufacturer B and inserts his personal smart card 102 to connect to the same ISP. If both manufacturers A and B have agreements with the desired ISP, then the process described above is carried out. The NC client device 101 is linked to the ISP through the relationship server database 112 as long as the NC client manufacturer has an agreement in place that matches the ENTERPRISE_ID coming from the smart card 102. If manufacturer B does not have an agreement with the desired ISP, then the NC client B is unable to connect to the ISP.

According to the present invention, a single NC client 101 may include authorization for several ISPs. According to an embodiment, the smart card 102 supports multiple ENTERPRISE_ID entries so that the user can purchase a combination smart card 102 with multiple ISPs accounts on it, in which case the NC client 101 prompts the user to choose to which ISP to attempt connection. According to another embodiment, when the NC client 101 dials the relationship server 111, all POP (Point of Presence) information for all the ISP partners that NC client manufacturer has is loaded into RAM 201. Therefore, one user with an ISP A smart card can use the NC client 101 having the correct contact information for ISP A. Another user with an ISP B smart card can subsequently use the NC client 101 having the correct contact information for ISP B.

Managed access requires the NC 101 to call a relationship server 111 when a blank card is inserted or the NVRAM/RAM contents are null and download appropriate initialization values based on the ENTERPRISE_ID. These contents are certified with a private key that only the manufacturer or trusted root authority holds. Furthermore, the relationship server 111 downloads a certified ISP public key.

Next, the NC device 101 calls the ISP and completes the registration process. The ISP's registration procedure writes home URL, DNS IP addresses, mount point and other appropriate information to the smart card 102 certified by the ISP. In other words, the ISP completes this process by placing a certificate on the smart card 102 that can be used to certify the contents and that only the ISP could have written the contents. The next time the NC 101 is turned on and the smart card 102 inserted, the NC 101 validates the contents of the smart card 102 by using the public key found

in the ISP certificate, validates the ISP public key by using the public found in the ROM. Thus, the manufacturer is the root of the entire certification hierarchy. When the NC client **101** boots, it reads the contents of the smart card **102**, uses the certificate to verify the contents and uses the public key stored in ROM **202** to verify the certificate.

The method carried out by the NC client device **101** using the managed access software according to the present invention is illustrated in FIGS. **3** through **10** (NC flow charts **1** through **8**). The method starts at step **1001** when the NC client device power switch is turned on. If at any time during the method illustrated in NC flow charts **1** through **8** the user's smart card **102** is pulled out of the NC client device **101**, then the method for managed access returns immediately to step **1001**.

At step **1002**, the NC client device **101** checks to see if a smart card **102** is inserted into the NC's smart card slot. If no smart card **102** is inserted, then the managed access software continues to look for the smart card **102** at step **1002** until it is inserted. At optional step **1003**, if there is a Personal Identification Number (PIN) associated with the smart card **102**, the NC client device **101** asks for the user's personal identification number and compares it with the PIN on the smart card **102**. If the PINs do not match, then the process stops. However, if the PINs do in fact match, then the method proceeds to step **1004**, if the smart card ENTERPRISE_ID matches an ENTERPRISE_ID found in the nonvolatile memory **203** of the NC client device **101**, then the method proceeds to step **1005**. If there is no match between the ENTERPRISE_ID on the smart card **102** and that found in NVRAM, then the method according to the present invention dials a relationship server **111** at step **1007** in NC flow chart **2**.

When delivered to the NC client **101** by the relationship server **111**, the root ISP certificate is written to NVRAM **203** or RAM **201** so as to enable user roaming to different NC client devices **101** authorized to connect to the same ISP **109** without depending on the same root public key being stored in all ROMs as the root authority. The certificate controlling usage of any given NC client **101** is created by the root authority whose public key is stored in the NC clients' ROM **202**. All root ISP certificates are created by the root authority and are delivered to the relationship server's database **112**. The smart card **102** contains information that is associated permanently with a particular user, and is not subject to the user's location. This includes, for example, the user's current home URL (universal resource locator), and the NFS/CSFS mount point. Information that is associated with the location of the client is stored in the NC client's RAM **201** and/or NVRAM **203**. This includes, for example, the ISP's IAP connect matrix and the DNS (domain name server).

The NC client **101** will store the connection details regarding the last successful ISP connection in NVRAM **203** because the NC client **101** must be able to cope with a power cycle without calling the relationship server **111**. Upon restarting, if the NC client **101** has valid connection information already stored in NVRAM **203**, the user will be prompted to specify whether or not the NC client **101** may use the connection information already stored in NVRAM **203** to connect to the IAP **105**. In general, if the NC client **101** has moved to a different telephone number, the user will answer "no" and will force the NC client **101** to call the relationship server **111** and to download local telephone and IAP connection information. This allows the user to prevent an NC client **101** which was previously used to connect to a distant IAP from dialing a non-local telephone number in order to connect to the same distant IAP **105**.

The test performed in step **1004** will be false if the smart card **102** does not contain an ENTERPRISE_ID (therefore has an ENTERPRISE_4ID of zero), if there is no ENTERPRISE_ID found in non-volatile memory **203**, or if the smart card **102** and the nonvolatile memory of the NC client device **101** store different ENTERPRISE_IDs. However, in the case of a match, the method proceeds to step **1005** at which a cryptographic verification of the smart card contents is performed using an Internet Service Provider (ISP) usage certificate found in nonvolatile memory **203**.

Every NC client **101** has either the manufacturer's or distributor's public key or the public key of trusted authority written into the ROM **202**. One example of such a trusted authority is the author of the managed access software according to the present invention which is provided to the relationship server **111**, the ISP **109**, and the NC client **101**. The public key which is written in ROM **202** serves as the root authority for verification of the certificates, and is therefore referred to as the root public key. The root public key must be stored in ROM **202** in order to guarantee its integrity; because the ROM **202** cannot be overwritten or altered, its contents are deemed safe. The public key stored in ROM **202** is the root public key responsible for verifying the signatures on all issued information or certificates from the root authority, such as the NC client manufacturer, the NC client distributor, or the managed access software author or distributor.

Before using information on the smart card **102**, the NC device **101** will verify the contents of the smart card **102** using the cryptographic signatures appended to the contents. Although any information to be stored in the RAM **201** or NVRAM **203** includes a digital signature portion, this digital signature is used only once for verification at the time of writing. Assuming that the digital signature checks at the time of writing to RAM **201** or NVRAM **203**, the digital signature appended to RAM or NVRAM contents is then discarded. The inside of the NC client **101** is deemed to be tamper proof for the purposes of the NC client's security requirements, and therefore all digital signatures for the RAM or the NVRAM contents may be discarded once verified and the contents are written to the RAM **201** or NVRAM **203**.

In the preferred embodiment, the ISP usage certificate is authenticated at the time that it is delivered from the relationship server **111** using the root public key; therefore, the ISP usage certificate need not be authenticated each time it is used if the integrity of the nonvolatile memory is trusted. However, step **1006** in NC flow chart **1** illustrates an optional step of authenticating the ISP usage certificate retrieved from nonvolatile memory **203** using the root public key retrieved from ROM **202** after the ISP usage certificate has been used to further protect against tampering with non-volatile memory, such as installing a certificate not signed by the root authority.

The root public key is typically written by the NC client device manufacturer at the time of manufacture and stands as the root authority for authentication and verification of signatures on the NC client device **101**. If either of the authentications carried out in steps **1005** or **1006** fail, then either the smart card **102** contents or the ISP certificate are not valid, and therefore should not be used by the ISP to provide services. If the ISP usage certificate retrieved from the nonvolatile memory **203** is unsuccessfully authenticated, then the user is prompted at step **1042** in NC flow chart **8** for permission to reprogram the smart card **102**. The user is also prompted for permission to reprogram the smart card **102** at step **1042** if the smart card **102** contents were unsuccessfully

authenticated at step **1005**. If the user grants such permission, then smart card **102** is reprogrammed at step **1043**. When the smart card **102** contents corresponding to the ISP are reprogrammed at step **1043**, it is written so as to contain only the ENTERPRISE_ID of the ISP. After reprogramming the smart card **102**, the method proceeds to step **1007** in NC flow chart **2**, at which the relationship server **111** is contacted.

However, assuming both cryptographic verifications at step **1005** and **1006** are carried out successfully, then the method continues to step **1023** on NC flow chart **5**, where the NC client device **101** checks its RAM to determine if there is an Internet Access Provider (IAP) matrix corresponding to the ENTERPRISE_ID which was retrieved from the smart card **102**. If there is no IAP matrix for the ISP designated by the smart card ENTERPRISE_ID, then the relationship server **111** must be contacted at step **1007** in NC flow chart **2** to provide the appropriate IAP connection information. However, if the IAP matrix corresponding to the ENTERPRISE_ID is found in a nonvolatile memory **203**, then the method proceeds to step **1024**, at which the local IAP Point of Presence (POP) telephone number that is in the IAP matrix within nonvolatile memory **203** is dialed by the NC client's modem.

At step **1025**, the NC client **101** runs the dial-up script to connect to the ISP. Then at step **1026** the NC client **101** transmits its username/password pair to the IAP **105**. The dial up script is run first, the script tells the NC client **101** what pieces to deliver to the IAP. For example, the dial up script tells the NC to dial the IAP phone number, then wait for the login prompt, feed the username, wait for the password prompt, then feed the password. If the NC successfully connects to the ISP at step **1027**, then the user and the ISP interact as specified initially by the ISP at step **1028**. However, if the connection between the NC and the ISP is not established, then the NC disconnects from the ISP and dials the relationship server **111** at step **1007**. When a root authority (an NC client manufacturer or distributor) breaks a relationship with an ISP partner, the ISP **109** surrenders all managed access software according to the present invention, thereby rendering their "managed access" service useless. If an NC client manufacturer or distributor terminates an agreement with a partner ISP **109**, then because the stale ISP access information is still held in the NVRAM **203** of the NC client **101**, the NC client **101** will nonetheless attempt to connect to the defunct ISP service. The ability to disable the managed access software is necessary because an IAP matrix may be held in NVRAM **203** for a long period of time. Even if the NC client **101** is powered down for a long period of time, upon restarting the NC client **101** will load the stale IAP matrix from NVRAM **203** and attempt to connect to the unauthorized ISP. In this event, when the NC client **101** attempts to connect to the ISP **109**, the connection fails and a call to the relationship server **111** is necessitated. If the manufacturer breaks a business agreement with an ISP, the managed access software used by the ISP is rendered ineffective by the relationship server **111** and connection between the NC and the ISP cannot be established. Under these circumstances, the NC is forced to dial the relationship server **111** so as to retrieve the connection information for a new ISP partner chosen by the NC client device manufacturer. This call to the relationship server **111** results in the initial data for a new ISP partner and associated IAP matrix being downloaded.

At step **1028** after the NC to ISP connection has been established, the initial Universal Resource Locator (URL) retrieved from the smart card **102** and the smart card serial number (if requested by the ISP) are transmitted to the ISP.

The branch at step **1028** illustrates that there are two separate procedures carried out by the ISP depending upon the state of the user's smart card **102**. One procedure beginning at step **1029** of NC flow chart **6** corresponds to the registration of the user with the ISP; this branch is taken when the user's smart card **102** contains preliminary registration information written by the relationship server **111**. The other branch beginning at step **1036** of NC flow chart **7** corresponds to the interaction between the ISP and the user after the user has been successfully registered. Therefore, a user ISP account has already been established, and the user's smart card **102** contains information written by the ISP. Therefore, branch G corresponds to ISP registration and branch H corresponds to ISP service provision. When the relationship server **111** had written the ISP initial URL smart card contents, the relationship server **111** did not provide any information which allowed the user to receive services from the ISP or to be billed by the ISP. The relationship server **111** had only provided enough information to contact the ISP registration URL and then once the initial connection to the initial URL is established, the ISP interacts with the user in the final steps of registration outlined in branch G.

These steps of user/ISP interaction, such as provision of a credit card number and establishment of a user password, are carried out at steps **1030**. At step **1031**, the ISP stops the registration if any of the user's information does not check, for example if the user provides an incorrect credit card number. However, assuming that all the user's data checks out, then the ISP proceeds to step **1032** at which point the NC client **101** receives ISP specific account data into the RAM **201** of the NC client device **101**. This account information enables the user to obtain services from the ISP and to connect to the user's home URL established for the user by the ISP. This ISP specific account data must be cryptographically verified before it can be written to a smart card **102**. Therefore, at step **1033**, the ISP specific account information received into RAM **201** from the ISP is verified using the ISP usage certificate found in nonvolatile memory **203**, which was provided by the relationship server **111**. Assuming that this verification passes at step **1034**, the ISP usage certificate in NVRAM **203** is optionally authenticated using the root public key found in read only memory **202**. In the preferred embodiment, step **1034** is omitted because the ISP usage certificate was authenticated when it was received from the relationship server **111**. If properly authenticated at step **1033**, then the ISP specific account data is written onto the ISP's smart card **102** section at step **1035**.

At step **1036** on NC flow chart **7**, the smart card ISP specific account data is transmitted to the ISP, along with the smart card serial number and the NC model number. This information will have just previously been written by the ISP if user registration with the ISP has just occurred in branch G. This transmission to the ISP includes the user's home URL, so that the user will now be connected to his home service URL for the ISP. If at step **1037** some problem with the user's specific account data is detected, for example, if the user's credit card no longer is valid, the ISP prompts the user to call the registration number at step **1044**. If the ISP determines at step **1037** that the NC client **101** needs a software patch in order to receive services, the ISP at step **1038** transmits the software patch and the NC client **101** receives it. If the NC client **101** does not need additional software, the method flows from step **1037** to step **1039** at which point the ISP facilitates interaction between the user and the ISP and provides services at step **1039**. Although step **1039** is illustrated as a single box, it represents whatever complicated back and forth communication between the NC

101, smart card 102, and ISP that the user and ISP are willing to participate in based on their relationship. At some point the user will pull out his smart card 102; and when this is detected at step 1040, the NC disconnects from the ISP at step 1041 and returns to the starting point of the NC method at step 1001.

Whenever, for any one of a variety of reasons, the NC client 101 must contact the relationship server 111, the NC's method for handling this begins at NC flow chart 2. At step 1007, the NC client device 101 dials the relationship server 111 typically via a toll free call. The same relationship server telephone number is used for NCs manufactured by all manufacturers. The flow proceeds to step 1008 at which point the NC client 101 transmits its manufacturer identification number from its nonvolatile memory and the ENTERPRISE_ID, if it exists, from the smart card 102 to the relationship server 111. If the smart card 102 is blank, zero is sent as the ENTERPRISE_ID. At step 1009, if the relationship server 111 determines that the NC client 101 needs a software patch to execute the procedures to be carried out while connected to the relationship server 111, then the NC client 101 receives the software patch into its RAM from the relationship server 111 at step 1010. If no software patch is needed by the NC client 101, the flow proceeds to step 1011. The relationship server 111 at step 1011 determines where to proceed next.

If the ISP designated by the smart card ENTERPRISE_ID is not authorized by the manufacturer specified by the NC client manufacturer ID stored in NVRAM, then the relationship server 111 disconnects from the NC client 101, and the NC client 101 stops because the users ISP is not authorized by the client device manufacturer and the relationship server 111 has disconnected from the NC client 101. If the relationship server 111 determines based upon the manufacturer ID and the smart card ENTERPRISE_ID that managed access is required and that the manufacturer has authorized the ISP specified by the ENTERPRISE_ID, then the relationship server 111 transmits (and the NC client 101 receives) a matrix of connect information corresponding to all Internet Access Providers (IAPs) for each ISP authorized by the manufacturer into the NC client's RAM at step 1012. The information delivered to the NC at step 1012 includes a digital signature from the relationship server 111 as well as a certificate from the manufacturer specifying the relationship server's public key. The certificate is authenticated using the root public key, and the IAP matrices are verified using the relationship server's public key at step 1012.

If managed access is not required based upon the manufacturer identification number, then at step 1011 the relationship server 111 sends the NC client 101 a list of the top 20 ISPs and corresponding IAP matrices at step 1018, prompts the user for selection of one of those ISPs at step 1019. When the user makes his selection at step 1020, the NC client 101 writes the selected ISP as the smart card ENTERPRISE_ID at step 1021 and writes the smart card initial registration contents for the selected ISP at step 1022. In the nonmanaged access scenario described by branch D, there is no signature requirements on the initial registration contents written to the smart card 102. If the internet service provider selected wants to use digital signatures after registration has occurred, it can do so. After the smart card initial registration contents are written at step 1022 in the nonmanaged access case, the NC client 101 disconnects from the relationship server 111 at step 1017.

In the managed access case described by branch E, once the matrix of Internet Access Providers for each ISP is received into the NC client's RAM at step 1012, the smart card contents for the selected ISP are verified using an ISP usage certificate found in NVRAM 203. If the smart card contents pass the cryptographic verification of step 1013 then the NC client 101 disconnects from the relationship server 111 at step 1017. If the cryptographic verification fails at step 1013, then the NC client 101 receives an ISP certificate into NVRAM from the relationship server 111 at step 1014. The cryptographic verification at step 1013 will fail if the ISP usage certificate in the NC client's NVRAM 203 is stale or, in other words, is the certificate for another ISP other than the one specified by the smart card ENTERPRISE_ID. After the NC client 101 has received the ISP usage certificate into the NVRAM 203 at step 1014, the NC client 101 authenticates the, ISP usage certificate at step 1015 using the root public key found in ROM. If the NVRAM ISP usage certificate does not pass the verification in step 1015, then it is deleted from nonvolatile memory 203, and the NC client 101 stops. (Alternatively, the ISP usage certificate is received into RAM at step 1014, authenticated and written to NVRAM upon successful authentication at step 1015.)

If the authentication at step 1015 passes, the NC client 101 receives the initial registration contents for the ISP and writes them to the smart card 102 and at step 1016. The NC client 101 then disconnects from the relationship server 111 at step 1017 and the method progresses to step 1023 in NC flow chart 5. At step 1023, the NC again searches for an IAP matrix corresponding to the newly authorized ISP designated by the recently written smart card ENTERPRISE_ID.

According to the present invention, the ROM 202 in each NC client 101 contains the telephone number of the relationship server 111, 1-800-RELATIONSHIP. Upon initially booting up, each NC client 101 must call the relationship server 111 which will manage the NC client's access of the partner ISP 109. This implies that ROM cards 202 are country specific since 1-800 toll free numbers apply to only to the United States.

The relationship server 111 issues certificates binding the names of ISPs 109 and other entities to their corresponding public keys. For those ISPs that the root authority authorizes to connect to its NC clients, the root authority computes and appends its digital signature to the relationship server's ISP certificates. The root public key in each NC client's ROM 202 is therefore used to verify the root authority's authorization of the ISP. Certificates and signatures issued by any entities will be verifiable via a series of certificates leading back to the root authority. This handles the verification of certificates that were not issued directly by the root authority, as long as the certificate issuer can be traced back following a chain of issuer names to the root authority.

The relationship server 111 issues ISP name/public key certificates (signed by the relationship server 111) binding ISPs 109 and other entities to their associated public keys. In the presently preferred embodiment, standard X.509 v1 or v3 certificates are used. The contents of these certificates includes the certificate version number, serial number, validity period, relationship server name, ISP name, ISP public key, and relationship server signature portion. If X.509 v3 certificates are used, the user defined field can be used to provide a URL link to a web page controlled by the relationship server 111 containing a security policy statement covering the valid use of the certificate. The serial numbers of these ISP name/public key certificates issued by the relationship server 111 are sequential and are therefore unique for each ISP. According to the present invention, the serial number of the relationship server ISP name/public key certificate is the enterprise identification number (ENTERPRISE_ID) uniquely associated with the ISP.

The relationship server **111** delivers these ISP name/public key certificates to the various root authorities. If a root authority wishes to authorize usage of its NC clients to connect to the ISP **109** specified in an ISP name/public key certificate, then the root authority computes and appends its digital signature to the ISP name/public key certificate, thereby creating a root ISP certificate. Each root authority sends its root ISP certificates back to the relationship server **111**. The relationship server **111** distributes these root ISP certificates to the NC clients of the root authority as will be described below.

The relationship server **111** maintains a database **112** which contains a list of all ISP names, ISP registration servers, and local POP (point of presence) telephone numbers. Because all NC clients **101** initially call the relationship server **111**, the relationship server's database **112** must contain the details of all ISP registration servers and POP telephone numbers for all areas. For those ISPs that have multiple IAP partners, the relationship server's database **112** also holds call matrices which list all IAPs and corresponding POPs which provide access to the ISP.

The methods executed by the relationship server **111** according to the present invention are described in the relationship server flow charts **1** and **2**. At step **2001**, the NC dials the relationship server **111**. At step **2002**, the relationship server **111** accepts the connection from the NC. At step **2003**, the relationship server **111** determines whether the not the NC client **101** needs a software patch in order to continue. If so, the relationship server **111** transmits the software patch at step **2004**. If there is no need for a software patch, then the relationship server **111** proceeds to step **2005** at which it receives the NC manufacturer identification number and the ENTERPRISE_ID (if it exists). If no ENTERPRISE_ID exists on the smart card **102** inserted into the NC client **101**, the relationship server receives an ENTERPRISE_ID of zero. The relationship server **111** uses the manufacturer identification number and the enterprise identification number to access the relationship server database **112** at step **2006** so as to determine whether or not managed access is required at step **2007**.

If the manufacturer specified by the manufacturer identification number does not place limits on which ISPs to which its NCs can be used to connect, then managed access is not required and the relationship server **111** transmits the top **20** ISPs and corresponding IAP matrices that are found in the relationship server database **112** at step **2015**. Then the relationship server **111** disconnects from the NC at step **2014** and then stops.

However, if at step **2007** the relationship server database **112** indicates that managed access is required, then the relationship server **111** proceeds to step **2008**, where the relationship server **111** checks its database **112** to determine whether or not the manufacturer has authorized connection of the NC client device **101** to the specific ENTERPRISE_ID transmitted to the relationship server **111**. If the ISP is not authorized by the manufacturer, the relationship server **111** disconnects from the NC at step **2014** and stops. However, if the manufacturer has authorized the ISP, then the relationship server **111** then transmits the matrix of IAPs corresponding to all ISPs authorized by the manufacturer at step **2009**.

If the NC at step **2010** in relationship server flow chart **2** indicates that it needs an ISP certificate for the ISP corresponding to the ENTERPRISE_ID, then the relationship server **111** transmits the ISP usage certificate at step **2011**. At step **2012**, if the NC determines that it needs initial registration contents for the ISP, then those contents are transmitted at step **2013** to the NC client **101** by the relationship server **111**. In any of these cases, the relationship server **111** then disconnects from the NC at step **2014** and stops.

According to the present invention, strong cryptographic authentication of an ISP **109** is required before allowing the ISP **109** to update the contents of the smart card **102**. In the presently preferred implementation, this is performed using standard SSL (secure sockets layer). The requirement that the ISP **109** compute and append a digital signature to the data it is writing to the smart card **102** is accomplished using non-proprietary protocols and software existent at both the NC client **101** and the ISP **109** ends.

According to the present invention, the addition of strong authentication to the NC client **101** does not require the storage of private keys and accompanying processing resources on the smart card **102**. The NC client **101** architecture according to the present invention requires only the verification of digital signatures, but does not require the generation of the NC client's own digital signatures; and therefore only requires the storage of public keys on the NC client **101**.

The IAP/ISP flow charts **1** and **2** describe the anticipated way that a typical IAP **105** and ISP will register a user and then will interact with the user once registered. When the NC client device **101** dials a local IAP telephone number at step **3001**, the IAP **105** receives a username/password at step **3002** necessary to gain access to the internet through the IAP **105**.

According to an embodiment of the present invention, the username/password pairs required to log on to the ISP **109** are written to NVRAM **203** or RAM **201**. Alternatively, according to the present invention, the NC client **101** supports an IAP matrix that is split between client device memory (NVRAM **203** and RAM **201**) and the smart card **102**. In the preferred embodiment of the present invention, the entire contents of the IAP matrix is placed in NVRAM **203** or RAM **201**. This preferred embodiment has the advantage that only ISP information is written to the smart card **102**; therefore, no IAP information is written to the smart card **102**. In this preferred embodiment, the username/password combinations are associated with specific telephone numbers. For example, if a user with an NC client **101** in his home has local POPs stored in the NVRAM **203** of his NC client **101** went from IAP A went across country and used an NC client **101** with POPs for IAP B, no call to the relationship server **111** is necessary because the NC is already fully enabled to connect to the IAP B.

At step **3003**, the URL transmitted to the IAP **105** by the NC client **101** from the smart card **102** will connect the NC either to the user's home page or to the ISP registration page. If the smart card URL was written by the relationship server **111**, the user has only completed the first phase of registration and must still register with the ISP. In this case, the smart card URL will specify a connection to the ISP registration page. However, if the smart card URL specifies a connection through the IAP **105** to the user's home page, then the user has already performed both phases of registration.

According to another aspect of the present invention, the smart card **102** includes a serial number which is readable by the ISP **109**. When the ISP initial URL must include the smart card serial number, the NC client **101** appends the smart card serial number to the end of the URL. If the manufacturer's serial number is needed in the ISP initial URL, the NC client **101** appends its unique serial number to the URL stored in the NC client's NVRAM **203**.

The smart card serial number can be used by the ISP **109** to authenticate or audit the initial URL connection to the ISP **109**. The ISP **109** can also use techniques to append information to the end of the URL that it downloads to the smart card **102**. In other words, when the ISP registration system creates the initial URL, the ISP **109** could create an initial URL such as the following:

http:/server/cgi-bin/login.cgi?username=BOB&password=RANDOM

The NC client **101** issues this initial URL to cause a connection to the the ISP's registration web page that may used to register and authenticate the user. No requirement is placed on the form of the initial URL issued by the relationship server **111** by managed access software according to the present invention. The ISP **109** has a great deal of flexibility as to how it operates the NC client **101**. The NC client **101** determines how to operate based partially upon the contents of the smart card **102**. For example, if the ISP **109** wants NFS to be used for booting, a dedicated tag is allocated and assigned the value "nfs" on the smart card **102**. Other types of file systems can be used by assigning different values to the allocated tag. The managed access software according to the present invention does not mandate the type of file system that the NC client **101** must use. The ISP **109** makes the choice of the file system based on the types of file systems supported by the NC clients that the ISP **109** wants to support. Therefore, the ISP **109** may be required to support more than one file system protocol if it is interested in supporting NC clients from various manufactures that do not all support any single common file system type.

If the registration URL has been sent to the IAP **105**, then the ISP interacts with the user at step **3004** to establish credit card billing and account data as provided for in the ISP registration page, and to establish a user password, if desired. At step **3005**, the ISP determines whether the user's credit card is valid. If not, it stops. If the credit card is valid at step **3006**, the ISP creates user specific account data such as account balances, ISP usage credits of various types which will vary from ISP to ISP. At step **3007**, the ISP creates a digital signature of the user's specific account data using the ISP's private key. At step **3008**, the ISP transmits to the NC client **101** the user specific account data along with its digital signature to the NC.

After registration, the ISP transfers the user to his home URL, which was included in the user specific account data and validates the user at step **3009** in IAP/ISP flowchart **2** using the password established for the user during registration at step **3004**. If this authentication of the user fails, then the ISP transmits a command to the NC to prompt the user to call the ISP's registration number at step **3013**. If the validation passes, then at step **3010** the ISP determines whether or not the NC needs a software patch to interact with the ISP at step **3010**. If no software patch is needed, then the ISP interacts with the user at step **3012**. If a patch is needed, then the ISP transmits it at step **3011** before interacting with the user at step **3012**.

FIG. **15** illustrates some of the preferred contents of the various memory devices associated with an NC, and also shows which entities are intended to write the various contents in the various fields. The relationship server telephone number and manufacturer serial number in NVRAM are written by the manufacturer, as indicated by the "M" characters in the field **1501**. All other fields of the NVRAM are written by the relationship server **111**, as indicated by the "RS" characters in the field **1501**. The IAP matrices in RAM corresponding to all ISPs is written by the relationship server **111**, as indicated in the "RS" in field **1502**. Obviously, the RAM also includes various transient program code and data (not shown) written by the NC and the ISP as well. The root authority public key in ROM is hard-coded, and is not writeable by any entities, as indicated by the "*" in the field **1503**. The smart card ENTERPRISE_ID may either be written by the relationship server **111** or may be hard-coded, as indicated by the "RS,*" shown in the field **1504**. The other smart card variables may be written by the relationship server **111** or the ISP, as indicated by the "RS, ISP" in the field **1504**.

The managed access system according to the present invention accommodates several different alternatives for handling ISP connectivity. According to one alternative, the smart card **102** supports multiple access points for each ISP in the form of an array of POP or IAP telephone numbers for each ISP **109**. According to another alternative, it supports separating the IAP information between the smart card **102** and NVRAM/RAM. In particular, the username/password pair is placed on the smart card **102**, and the rest of the IAP matrix is placed into NVRAM **203**. In the preferred embodiment, both the username/password pair and the rest of the IAP matrix are placed into NVRAM **203**. The smart card contents are digitally signed to protect the ISP clients and NC device manufacture.

The NC device uses a certificate based algorithm to verify the writer of the smart card contents before using the information on the smart card **102**. According to the present invention, the ISP **109** is permitted to write the information on the smart card **102** that it controls and the relationship server **111** is permitted to write information to the NVRAM **203** that enables the NC client **101** to verify the ISP **109**. The relationship server **111** initially stores on the smart card **102** the initial ISP registration URL and the NFS/CSFS mount point. The relationship server **111** writes the root ISP certificate to NVRAM **203**. This initial connect information was provided by the root authority to the relationship server **111** and is signed by the root authority. Before allowing this initial connect information to be stored onto the smart card **102**, the NC client **101** authenticates the origin of the initial connect information using the root public key stored in ROM **202** to authenticate the root signature on the initial connect information. Before allowing the ISP **109** to write account information onto the smart card **102**, the NC client **101** authenticates the ISP's signature appended to the account information using the ISP public key found in the ISP certificate in NVRAM **203** and authenticates the ISP public key by verifying the root signature on the ISP certificate using the root public key found in its ROM **202**. After such authentication, the ISP **109** is permitted to rewrite the ISP URL and the NFS/CSFS mount point information. The ISP **109** may rewrite this connect information after the user has successfully registered with the ISP's registration system.

All data on the smart card **102** is written including the digital signature of the author of the data, so that the data's integrity can be verified. The combination of the telephonic dial-up process and the standard usage of strong authentication insures that only the relationship server **111** and the ISP **109** are writing to the smart card **102**. However, in order to allow this updating of critical information on the smart card **102** by other parties we require strong authentication of these entities. According to the present invention, this is accomplished using existing standard strong authentication mechanisms from the ISP **109** to the NC client **101**. For example, Secure Sockets Layer (SSL) version 3.0 using

RSA certificates is preferably used for authentication. The NC client **101** holds in ROM **202** a root certificate. The ISP **109** authenticates itself to the NC client **101**; however, the NC client **101** does not authenticate itself to the ISP. Because the NC client **101** does not add a digital signature to anything, it does not need to store and private keys. The NC client **101** is authenticated by virtue of the username/password pair that the ISP **109** may require for logging on to the ISP **109**.

The boot block employees a Type Length Value (TLV) semantics. Each entry contains a four byte type indicator, a two byte length indicator and a value. All data is stored in big-endian format. The boot block is a collection of files of a given size. The given sizes for each file is the same but not necessarily the same for each smart card **102**. In other words, one smart card **102** may have all 440 byte files and another may have 800 byte files. It is not necessary to specify the exact file size of an NC smart card **102** since this version of the boot block structure does not rely on a fixed file size. However, the structure of the directory is fixed. There is one index file that contains information to rest of the directory structure. Each smart card **102** supports the ability to read the file sizes and names from the cards. The NC client **101** is expected to use this information to determine the directory structure. While the file sizes are not fixed, there are file sizes that are initially more efficient then others and should make for a better choice; however, in the future these values may change.

A smart card **102** can hold one or more enterprise contents. An enterprise contents is the information for a particular ISP or corporate client. A unique ENTERPRISE_ID is associated with every enterprise contents. Therefore, the smart card **102** can be broken into individual enterprise contents each labeled by an ENTERPRISE_ID. An optional enterprise offset structure is held in the index file. An enterprise offset structure is used to quickly determine the ENTERPRISE_IDs found on the smart card **102**. This is useful if more then one ISP is written to the smart card **102**. By reading the enterprise offset structure, the client can quickly give the user the choice of which ISP he wants to use and the offset to where that ISP's boot block information is located. If enterprise offsets are not present, it can be assumed that only one ENTERPRISE_ID is located on the smart card **102**. In the consumer market, this may prove to be very useful when multiple ISPs are common.

The interpretation of the value is dependent upon the tag identifier. If the high bit of the first tag identifier byte is set, it indicates that the field is an "aggregate". Aggregate values consist of zero or more nested tagged field values with the same structure as above. This provides a mechanism for representing nested data types. The tag identifier of the outer nest environment defines the meaning of the inner tag identifiers. The inner tags may represent the either individual elements of an array, a sequence, or a set: that determination is left up to the individual applications.

Without the entire IAP matrix in NVRAM/RAM the smart card **102** would look like:

```
<BeginSignatureTag><len until signature tag>
<EnterpriseIDTag><4><num>
<AuthenticationUserNameTag><len><username>
<AuthenticationPasswordTag><len><passwd>
<ServerNameTag><len><nfs server>
<UserMountPointTag><len><rw mount>
<URLTag><len><url>
<ProxyTag><len><proxy ip>
<SignatureTag><len><long num>
```

The signature is enclosed by an BeginSignature tag and ended when the SignatureTag is reached. Everything except for the possible enterprise certificate is ignored outside of the signature tag. In other words, if the data is not surrounded by a signature it is considered garbage. The signature is formed from hashing the entire contents, with the obvious exception of the signature. The enterprise certificate is not stored on the smart card **102** when used with Managed Access.

A notable tag is the BlankSpaceTag tag. This tag is useful to allocate free space to allow growth in a given ENTERPRISE_ID before the next one starts. For example, to leave room for another IAP one would use:

<BlankSpace>.<length><space>

Since the POP phone numbers, enterprise certificate, and other information can be either in RAM/NVRAM or on the smart card **102**, it is important that the NC client **101** determines the appropriate action to take and finds the information in the appropriate place. If Managed Access is required by the NC Client hardware, the NC Client software must make sure an ENTERPRISE_ID matrix is stored in RAM/NVRAM. However, if Managed Access is not required, information on the smart card **102** is used in preference to the information in RAM/NVRAM.

If a value extends pass the end of a file, it continues into the next boot block file. In other words, if a signature is 550 bytes and the boot block files are only 440 bytes, the signature will extend to the next boot block file.

The contents stored in NVRAM/RAM are not specified or mandated according to the present invention since each NC client software ventor or manufacturer can determine its contents and access methods independently. No requirement is placed on the format of the RAM/NVRAM since the manufacturer's OS is free to read and write this information in anyway it finds most convenient; however, the format used to download these contents is standardized. A canonical form understood by both the downloading server and NC client **101** is necessary because the downloading server creates both smart card content packets as well as NVRAM/RAM content packets. For simplicity, the same format for both destinations (smart card **102** and NVRAM/RAM) is preferrably used.

When the downloading server creates the contents that it wants to write to the client, it uses a special MIME type to download the packet into the NC client **101**. The MIME type is called content_type: application/nc-smart card. A blank line followed by TLV formatted data follows. The first (optional) tag indicates the server status and indicates the contents that follow. The RAMContentTag or Smart card-ContentTag indicates the destination of the accompanying data.

Following the contents are two URLs used by the client to go to the next HTML page. A URL indicating successful completion is provided as well as one indicating an error. For example:

DONE_URL=<URL used for successfully completion>
ERROR URL=<URL used for some kind of error>
DONE_URL=http://my-registration-server/cgi-bin/register.cgi?done?username
ERROR_URL=http://my-registration-server/cgi-bin/register.cgi?error?username

For multiple ENTERPRISE_IDs (i.e. more than one ISP is downloaded), the EnterpriseMaxtixTag is used. However, the signatures are executed over individual ENTERPRISE_IDs and does not include the EnterpriseMatrixTag or contents. While the NC client **101** does not store and revalidate the signature for the NVRAM/RAM contents, they are required so the NC verifies that it is talking to an appropriate service that is allowed to write to it. Note, even though augmenting the NVRAM would not result in abuse of the NC box, denial of service could result as a result of HTML pages downloaded misinformation to NVRAM/RAM.

The NC client **101** is responsible for piecing the necessary parameters from NVRAM and the smart card **102** into a useful form that it can operate on. In other words, the IAP matrix as a whole is useful to keep together but it may come in pieces (e.g. username/password pairs from the smart card **102** and the rest from NVRAM). No requirements are made on this form according to the present invention.

The contents that are downloaded depend on the type of server the data is used on. In other words, the ISP for which the smart card **102** contents are created determines, in conjunction with the type of NC client **101**, what tags are required. The ISP will decide which type of file system is being used, for example.

When the client detects a need to call the relationship server **111**, it passes the manufacturer's serial number to the relationship server **111** and the ENTERPRISE_ID once it establishes the connection. If the NC client **101** is calling the relationship server **111** for the first time, it uses ENTERPRISE_ID zero. Thus the packet sent by the client to the relationship server **111** looks like:

<ManufacturerIDTag><len><xx.xx. . .xxxxxxxx>
<EnterpriseIDTag><4><0>

The relationship server **111** then takes the manufacturer serial number and looks up the supported ISPs for the NC client **101**. If it already has an ENTERPRISE_ID stored on the smart card **102** but needs updated RAM contents, it supplies the ENTERPRISE_ID found on the smart card **102**. If more then one ISP is available, the relationship server **111** downloads the full contents for both NVRAM and the smart card **102** in its packet, The relationship server **111** packages the multiple ISPs using the EnterpriseMatrixTag. Once the packet is received by the client, the NC client **101** can disconnect from the relationship server **111**.

When the smart card **102** is blank, the NC client **101** determines which ISP to write to the smart card **102** and NVRAM. If only one ISP is down loaded, it simply writes the one available ISP to the smart card **102** and NVRAM. If the NC client **101** cannot write all of the available ISPs to the smart card **102**, it must prompt the user to choose which ISP he/she wants to use. The chosen ISP is written to the smart card **102** and corresponding NVRAM contents is written to NVRAM. The packet received for NVRAM is also signed by the relationship server **111**, and although the signature is not stored by the NC client **101**, it is verified using the relationship server's public key before writing.

If the smart card **102** is not blank, the NC client **101** determines for which ISPs it must write the corresponding RAM contents to NVRAM. If none is available, an error should be returned to the user. Since the NC client **101** does not know what time zone it is in, the relationship server **111** will download date, time, and time zone information. This way, the rules, which are based on time, can be applied correctly. This implies that the relationship server **111** must relate time zones with area codes. Because through user prompting or A&I services, the relationship server **111** locates the relative location of the NC client **101**, it can easily store the time zone of all the possible locations in the database **112**. An example of the date, time, and time zone formats is as follows:

<DateTag><10><YYYY:MM:DD><TimeTag><HH:MM:SS>
<TimeZoneTag><2><zone number>

Every time the client receives a packet to write to the smart card **102**, it updates the index file with ENTERPRISED_ID(s) written to the smart card **102** and their offsets. Furthermore, the NC client **101** writes the version number to the index file. This is not known or dealt with by the registration server or relationship server **111**; it is completely handled by the client. An enterprise signature is created by performing a secure hash on the enterprise contents and encrypting it with the enterprise private key.

Rules give a time range for the use of an IAP **105** found in an IAP matrix. The format of the rule gives the high and low range for the time in which an IAP **105** should be used. For example, <RuleTimeTag><**4**><**1200,1700**>—means 12 pm to 5 pm. Phone numbers are stored in an ASCII string. For example:
<POPPhoneNumberTag><**7**><**6314100**>:

The manufacture's identification number is preferably stored in NVRAM. It is a composite of many different parts of the NC client **101** including: BIOS number, NC client number, and manufacture's identification number.

The parts consist of:

serial number version	8 bits
serial number type	8 bits
manufacture id	16 bits
model number	16 bits
BIOS version	32 bits
NCOS version	32 bits
serial number	variable size

The serial number version is simply the version of the format of the serial number itself. The serial number type is defined to be the type of the variable length portion of the serial number. For example, the variable length serial number could be derived from the Ethernet MAC address, a manufacturer assigned number, a Dallas chip assigned number, or assigned by the managed access software author. The manufacture identification number is a number assigned by the managed access software author for each manufacture

of an NC badged network computer. The model number is assigned by the manufacturer of the NC hardware platform. A model number represents the hardware configuration of the NC. The BIOS and NCOS version numbers are assigned by the managed access software author and are in the form of major.minor.patch.port where each component is 8 bits. The serial number is a variable length number designed by the manufacturer. It is variable length because the contents are not mandated.

To compose a serial number, the NC client software must combine pieces found in various places. The serial number version, serial number type, manufacture id, BIOS version and model number are placed into the ROM. The NCOS version number is put into the NCOS itself. Of course, this might also be in ROM or it maybe downloaded. The location variable length serial number depends on the type. If it is provided by the manufacturer, it is burned into NVRAM.

When transmitted in string form, each part is represented in a hexadecimal number separated by a dot. For example, 01.03.0001.0001.01030101.01030101.00000001

The alternative 1-800 number is used as a replacement for the 1-800-relationship server number found in ROM. It can either be stored in ROM, downloaded, or initialized on a new smart card **102**. Like other contents, the alternative 1-800 number must be signed. Therefore, it is proceeded by BeginSignatureTag and followed by a SignatureTag. It is signed by the private key used in conjunction with the public key stored in ROM. This is either the manufacturer private key or the trusted authority's private key depending on what public key is stored in ROM.

The alternative relationship number is stored in a boot block. The offset tag in the index file determines which boot block the alternative relationship number is stored. The index file holds the version number and an optional enterprise group tag. The EnterpriseGroupTag lists which enterprises are on the card and the offsets upon which to find them. This can be very useful when multiple ISPs are stored on one smart card **102**. The version number is written by the NC client **101** when it is initially written with contents. This implies that the manufacturer of the smart card **102** only needs to burn the serial number and boot block directory structure. The contents of the boot blocks are intially empty.

While the present invention has been described with reference to its preferred and alternative embodiments, those embodiments are offered by way of example, not by way of limitation. The foregoing detailed description of the invention has been presented for purposes of illustration and description. It is not intended to be exhaustive or to limit the invention to the precise form disclosed, and obviously many modifications and variations are possible in light of the above teaching. The described embodiment was chosen in order to best explain the principles of the invention and its practical application to thereby enable others skilled in the art to best utilize the invention in various embodiments and with various modifications as are suited to the particular use contemplated. Those skilled in the art will be enabled by this disclosure to make various obvious additions or modifications to the the embodiments described herein; those additions and modifications are deemed to lie within the scope of the present invention. It is intended that the scope of the invention be defined by the claims appended hereto.

What is claimed is:

1. A method for connecting a network computer client device (NC) to an internet service provider (ISP), the method comprising the steps of:

(a) dialing a relationship server;

(b) transmitting an NC manufacturer identification number to the relationship server corresponding to an NC manufacturer of the NC;

(c) receiving an authorized usage certificate for the ISP from the relationship server that includes a manufacturer's digital signature;

(d) performing a cryptographic verification of the authorized usage certificate for the ISP using an NC root public key; and

(e) connecting to the ISP if step (d) is successful.

2. A method as in claim **1**, further comprising the step of:

after step (a) and before step (c),

(f) transmitting an enterprise identification number from a smart card inserted into the NC corresponding to the ISP to the relationship server.

3. A method as in claim **1**, further comprising the step of:

before step (a),

(g) performing a cryptographic verification of a stale authorized usage certificate for an unauthorized ISP using the NC root public key;

(h) attempting to connect to the unauthorized ISP; and

(i) if step (h) is unsuccessful, proceeding to step (a).

4. A method as in claim **3**,

wherein step (g) includes the step of reading the stale authorized usage certificate from a non-volatile memory within the NC;

wherein step (c) includes the step of writing the authorized usage certificate to the non-volatile memory within the NC; and

wherein step (d) includes the step of reading the authorized usage certificate from the non-volatile memory within the NC.

5. A method as in claim **1**,

wherein step (d) includes the step of reading the NC root public key from a read only memory.

6. A method as in claim **4**,

wherein step (a) includes the step of reading a relationship server telephone number from the non-volatile memory.

7. A method as in claim **5**,

wherein step (b) includes the step of reading a manufacturer serial number from the non-volatile memory.

8. A method as in claim **1**, further comprising the step of:

after step (b) and before step (e),

(j) receiving an ISP list of all enterprise identification numbers corresponding to all internet service providers authorized by the NC manufacturer from the relationship server.

9. A method as in claim **8**, further comprising the step of:

after step (b) and before step (e),

(k) receiving an internet access provider connect matrix for each enterprise identification number in the ISP list from the relationship server.

10. A method as in claim **8**, further comprising the step of:

after step (j) and before step (c),

(l) receiving an ISP selection from an NC user indicating which internet service provider from the ISP list to which to attempt connection.

11. A computer readable storage medium comprising:

computer readable program code embodied on said computer readable storage medium, said computer readable program code for programming a computer to perform a method for connecting said computer (NC) to an internet service provider (ISP), the method comprising the steps of:

(a) dialing a relationship server;

(b) transmitting an NC manufacturer identification number to the relationship server corresponding to an NC manufacturer of the NC;

(c) receiving an authorized usage certificate for the ISP from the relationship server that includes a manufacturer's digital signature;

(d) performing a cryptographic verification of the authorized usage certificate for the ISP using an NC root public key; and

(e) connecting to the ISP if step (d) is successful.

12. A computer readable storage medium comprising computer readable program code as in claim **11**, further comprising the step of:

after step (a) and before step (c),

(f) transmitting an enterprise identification number from a smart card inserted into the NC corresponding to the ISP to the relationship server.

13. A computer readable storage medium comprising computer readable program code as in claim **11**, further comprising the step of:

before step (a),

(g) performing a cryptographic verification of a stale authorized usage certificate for an unauthorized ISP using the NC root public key;

(h) attempting to connect to the unauthorized ISP; and

(i) if step (h) is unsuccessful, proceeding to step (a).

14. A computer readable storage medium comprising computer readable program code as in claim **13**,

wherein step (g) includes the step of reading the stale authorized usage certificate from a non-volatile memory within the NC;

wherein step (c) includes the step of writing the authorized usage certificate to the non-volatile memory within the NC; and

wherein step (d) includes the step of reading the authorized usage certificate from the non-volatile memory within the NC.

15. A computer readable storage medium comprising computer readable program code as in claim **11**,

wherein step (d) includes the step of reading the NC root public key from a read only memory.

16. A computer readable storage medium comprising computer readable program code as in claim **14**,

wherein step (a) includes the step of reading a relationship server telephone number from the non-volatile memory.

17. A computer readable storage medium comprising computer readable program code as in claim **15**,

wherein step (b) includes the step of reading a manufacturer serial number from the non-volatile memory.

18. A computer readable storage medium comprising computer readable program code as in claim **11**, further comprising the step of:

after step (b) and before step (e),

(j) receiving an ISP list of all enterprise identification numbers corresponding to all internet service providers authorized by the NC manufacturer from the relationship server.

19. A computer readable storage medium comprising computer readable program code as in claim **18**, further comprising the step of:

after step (b) and before step (e),

(k) receiving an internet access provider connect matrix for each enterprise identification number in the ISP list from the relationship server.

20. A computer readable storage medium comprising computer readable program code as in claim **18**, further comprising the step of:

after step (j) and before step (c),

(l) receiving an ISP selection from an NC user indicating which internet service provider from the ISP list to which to attempt connection.

21. An apparatus for connecting a network computer client device (NC) to an internet service provider (ISP), the apparatus comprising:

(a) means for dialing a relationship server;

(b) means for transmitting an NC manufacturer identification number to the relationship server corresponding to an NC manufacturer of the NC;

(c) means for receiving an authorized usage certificate for the ISP from the relationship server that includes a manufacturer's digital signature;

(d) means for performing a cryptographic verification of the authorized usage certificate for the ISP using an NC root public key; and

(e) means for connecting to the ISP responsive to means (d).

22. An apparatus as in claim **21**, further comprising:

(f) means for transmitting an enterprise identification number from a smart card inserted into the NC corresponding to the ISP to the relationship server.

23. An apparatus as in claim **21**, further comprising the step of:

(g) means for performing a cryptographic verification of a stale authorized usage certificate for an unauthorized ISP using the NC root public key;

(h) means for attempting to connect to the unauthorized ISP; and

(i) means for invoking means (a) responsive to means (h).

24. An apparatus as in claim **23**,

wherein means (g) includes means for reading the stale authorized usage certificate from a non-volatile memory within the NC;

wherein means (c) includes means for writing the authorized usage certificate to the non-volatile memory within the NC; and

wherein means (d) includes means for reading the authorized usage certificate from the non-volatile memory within the NC.

25. An apparatus as in claim **21**,

wherein means (d) includes means for reading the NC root public key from a read only memory.

26. An apparatus as in claim **24**,

wherein means (a) includes means for reading a relationship server telephone number from the non-volatile memory.

27. An apparatus as in claim **25**,

wherein means (b) includes means for reading a manufacturer serial number from the non-volatile memory.

28. An apparatus as in claim **21**, further comprising:

(j) means for receiving an ISP list of all enterprise identification numbers corresponding to all internet service providers authorized by the NC manufacturer from the relationship server.

29. An apparatus as in claim **28**, further comprising:

(k) means for receiving an internet access provider connect matrix for each enterprise identification number in the ISP list from the relationship server.

30. An apparatus as in claim **28**, further comprising the step of:

(l) means for receiving an ISP selection from an NC user indicating which internet service provider from the ISP list to which to attempt connection.

* * * * *

EXHIBIT D

US005991271A

United States Patent [19]

Jones et al.

[11] Patent Number: 5,991,271

[45] Date of Patent: Nov. 23, 1999

[54] **SIGNAL-TO-CHANNEL MAPPING FOR MULTI-CHANNEL, MULTI-SIGNAL TRANSMISSION SYSTEMS**

[75] Inventors: **David C. Jones**, Louisville; **Youngho Lee**, Boulder; **Bruce A. Phillips**, Highlands Ranch, all of Colo.

[73] Assignee: **US West, Inc.**, Englewood, Colo.

[21] Appl. No.: **08/575,402**

[22] Filed: **Dec. 20, 1995**

[51] **Int. Cl.**[6] **H04J 1/00**

[52] **U.S. Cl.** **370/252**; 370/437; 370/487

[58] **Field of Search** 370/252, 430, 370/437, 464, 465, 480, 486, 490, 496, 333, 466, 467; 348/14, 15, 16; 379/414, 416, 417

[56] **References Cited**

U.S. PATENT DOCUMENTS

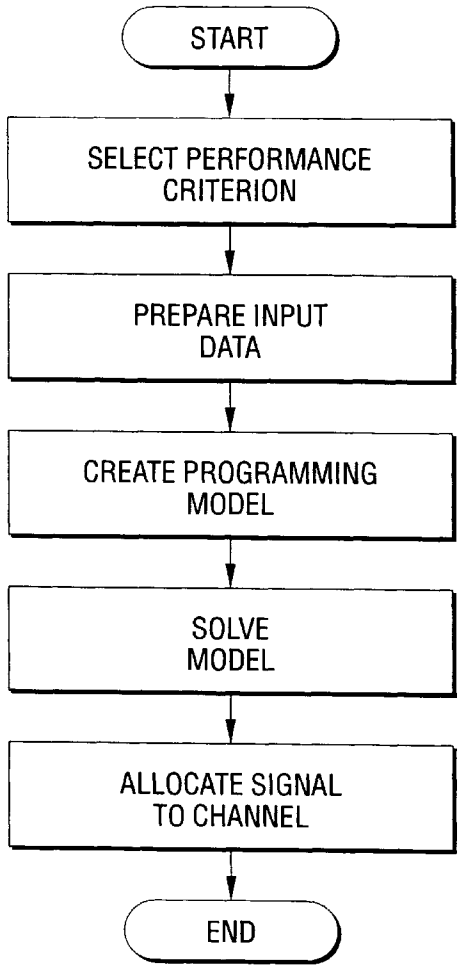
4,930,120	5/1990	Baxter et al.	370/487
4,947,459	8/1990	Nelson et al.	359/110
4,999,833	3/1991	Lee	370/390
5,375,123	12/1994	Andersson et al.	370/333
5,404,574	4/1995	Benveniste	455/33.1
5,512,937	4/1996	Beierle	348/14
5,534,914	7/1996	Flohr et al.	348/15
5,610,916	3/1997	Kostreski et al.	370/487

Primary Examiner—Alpus H. Hsu
Assistant Examiner—Kwang B. Yao
Attorney, Agent, or Firm—Brooks & Kushman P.C.

[57] **ABSTRACT**

A system and method for allocating signal types to transmission channels in a multi-channel, multi-signal transmission system uses one or more decision rules to determine a signal-to-channel mapping based on a predetermined performance criterion, such as signal-to-noise ratio (SNR), SNR margin, or target transport margin at a particular bit error rate (BER), rather than random assignment. The system and method improve overall performance of a transmission system carrying multiple signal types, such as telephony, compressed digital video, broadcast video, and low and high speed data. The decision rules are implemented over the entire transmission system to simplify recordkeeping and associated aspects of network operations.

19 Claims, 6 Drawing Sheets



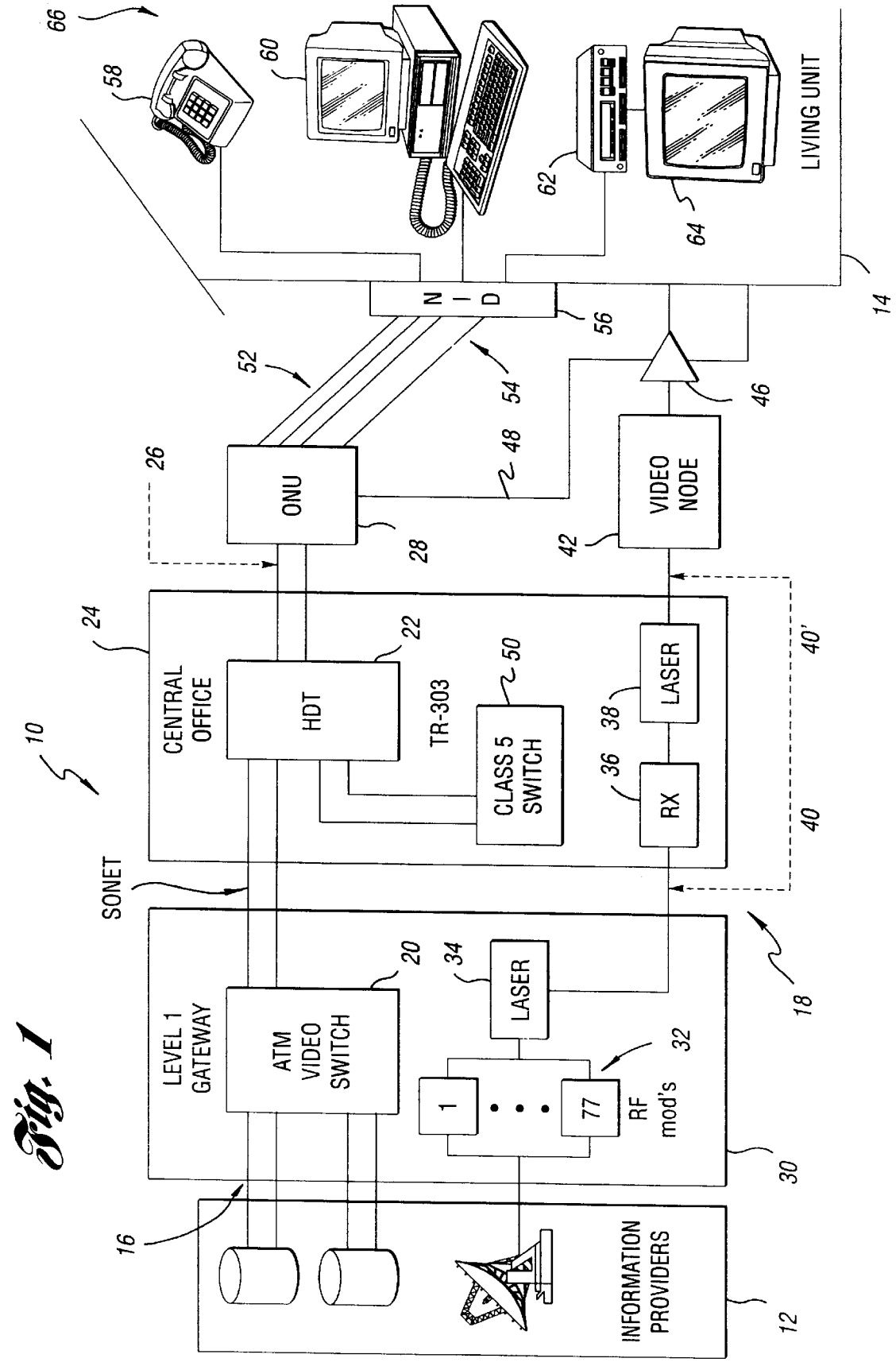

66
58
60
62
64
LIVING UNIT
14
N I D
56
52
54
46
48
26
ONU
28
VIDEO NODE
42
24
CENTRAL OFFICE
HDT
22
TR-303
CLASS 5 SWITCH
50
LASER
38
RX
36
40'
40
10
SONET
LEVEL 1 GATEWAY
ATM VIDEO SWITCH
20
LASER
34
1
77
RF mod's
32
18
30
16
INFORMATION PROVIDERS
12

Fig. 1

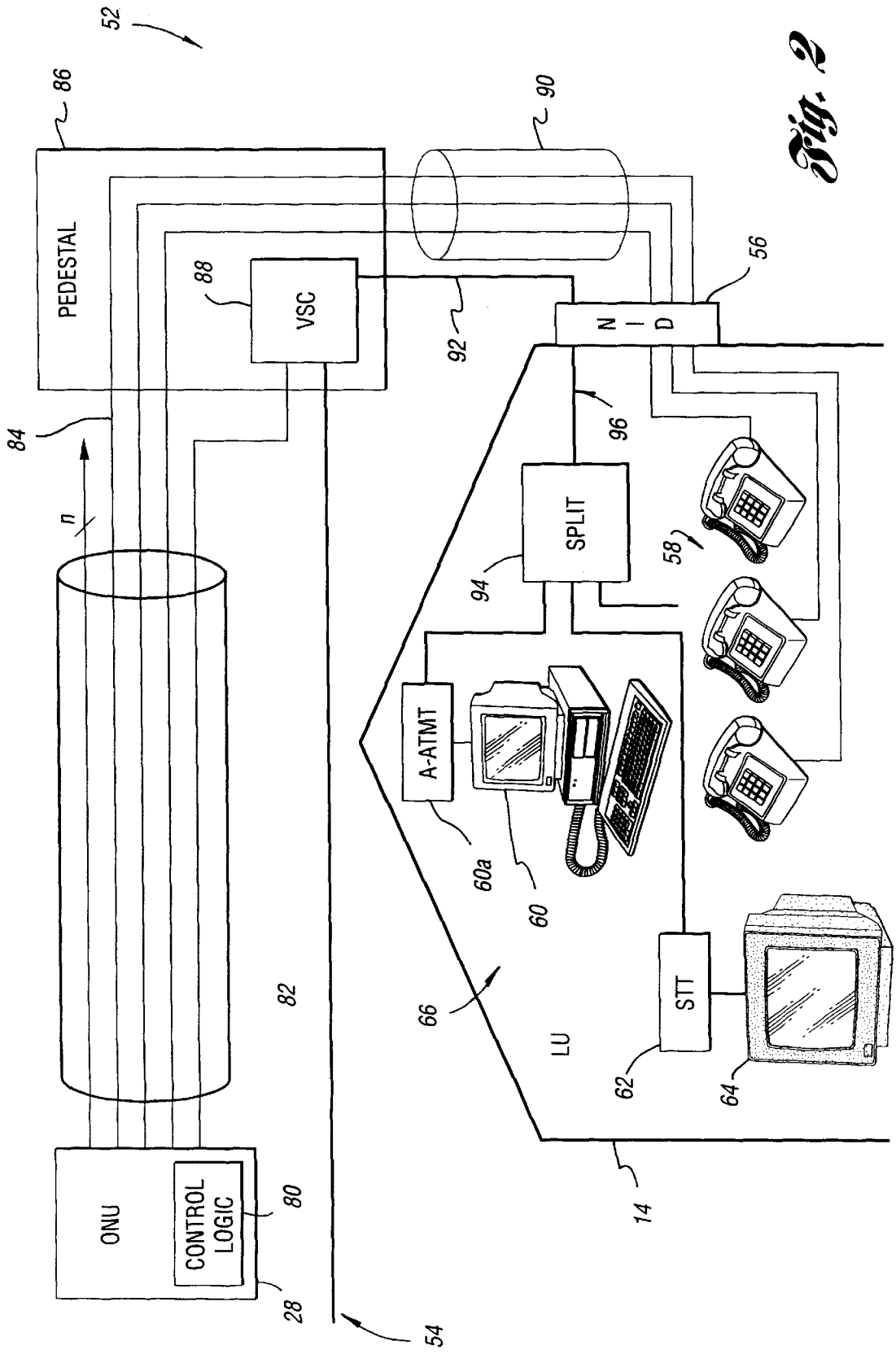
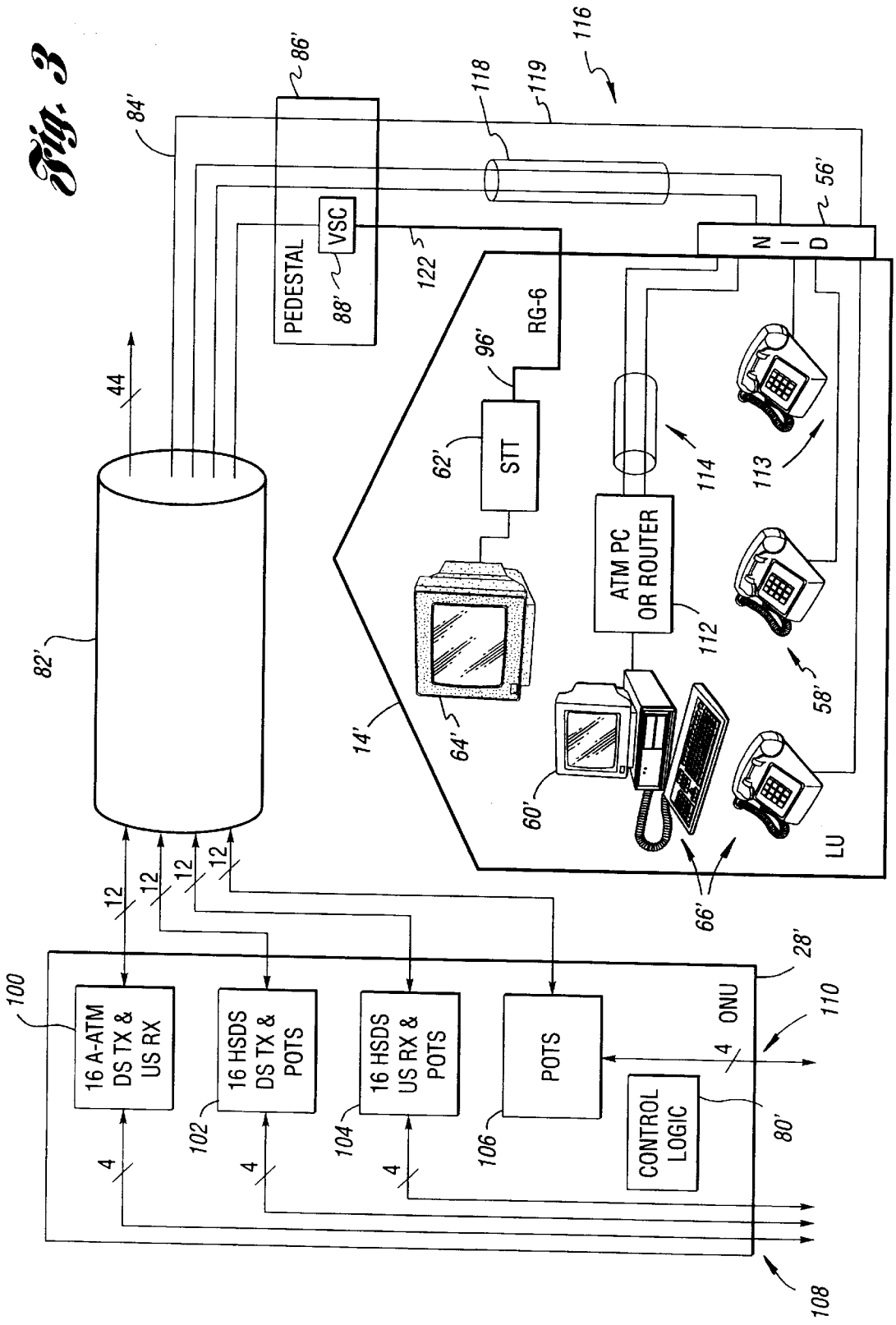

52
86
PEDESTAL
88
VSC
90
92
56
N I D
84
n
96
SPLIT
94
58
A-ATMT
60a
60
66
LU
STT
62
64
14
82
ONU
CONTROL LOGIC
80
28
54

Fig. 2

Fig. 3


84'
86'
118
119
116
56'
PEDESTAL
VSC
88'
122
N I D
RG-6
96'
62'
STT
44
82'
14'
64'
ATM PC OR ROUTER
112
114
113
58'
60'
66'
LU
12
12
12
12
100
16 A-ATM DS TX & US RX
16 HSDS DS TX & POTS
16 HSDS US RX & POTS
POTS
4 ONU
28'
110
CONTROL LOGIC
80'
102
104
106
4
4
4
108

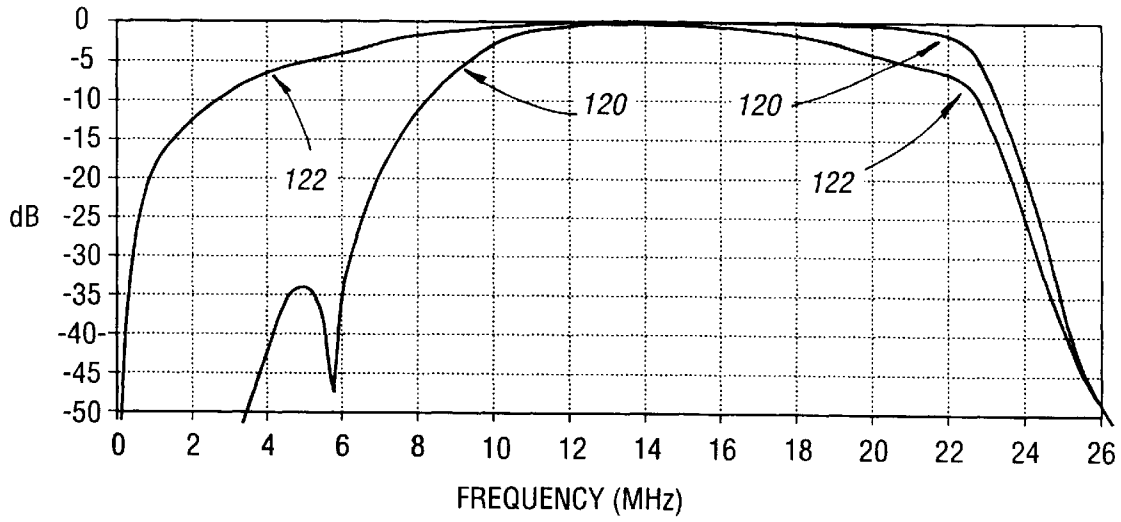

0
-5
-10
-15
-20
-25
-30
-35
-40
-45
-50
dB
0
2
4
6
8
10
12
14
16
18
20
22
24
26
FREQUENCY (MHz)
120
120
122
122

Fig. 4

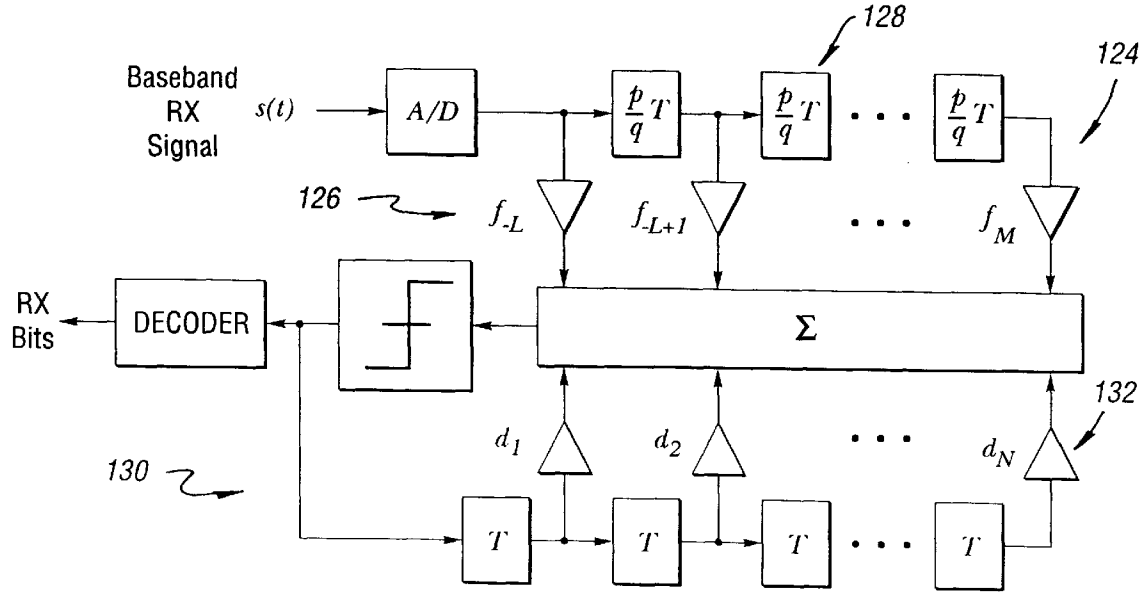

Baseband
RX
Signal
s(t)
A/D
$\frac{p}{q}T$
$\frac{p}{q}T$
$\frac{p}{q}T$
128
124
126
f_{-L}
f_{-L+1}
f_M
RX
Bits
DECODER
Σ
132
d_1
d_2
d_N
130
T
T
T
T

Fig. 5

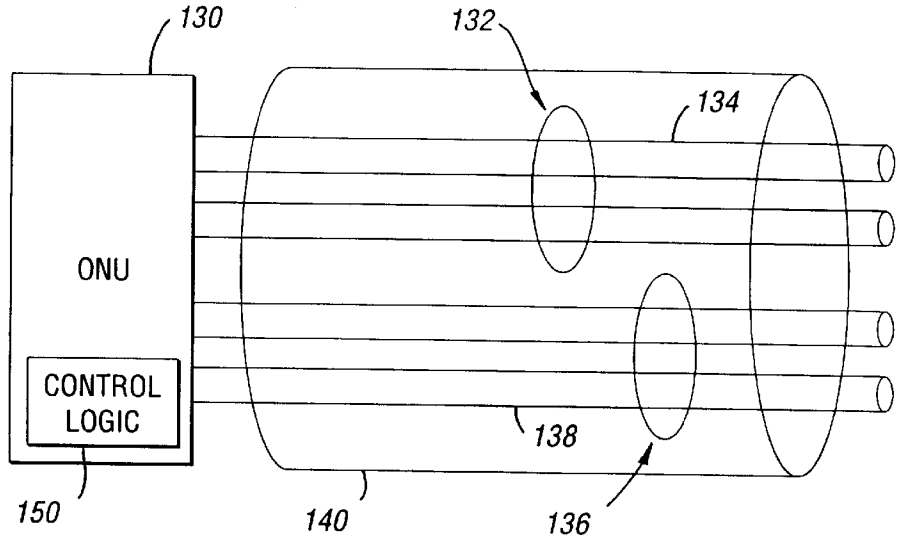


Fig. 6

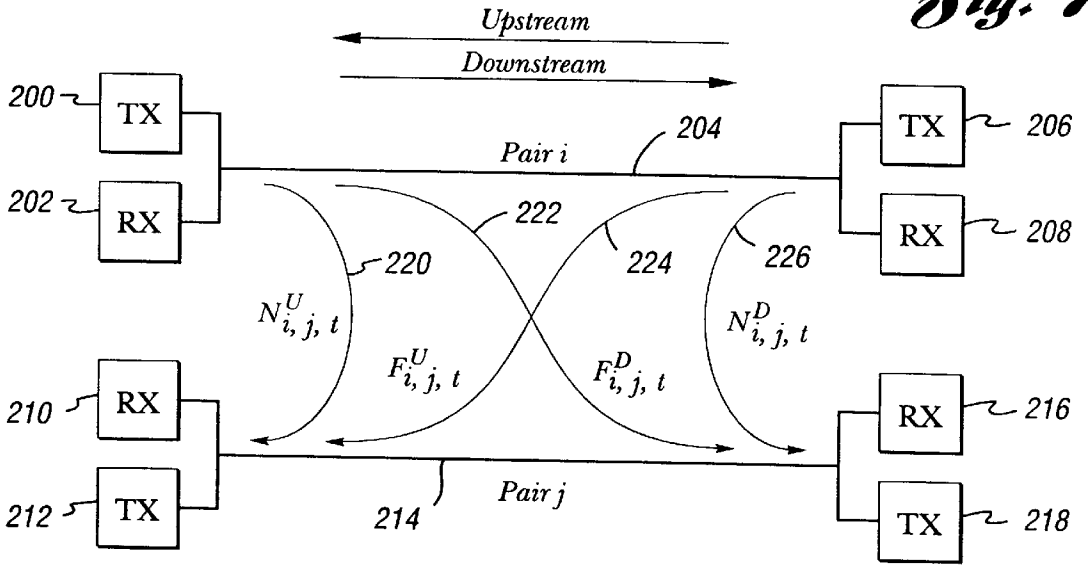


Fig. 7

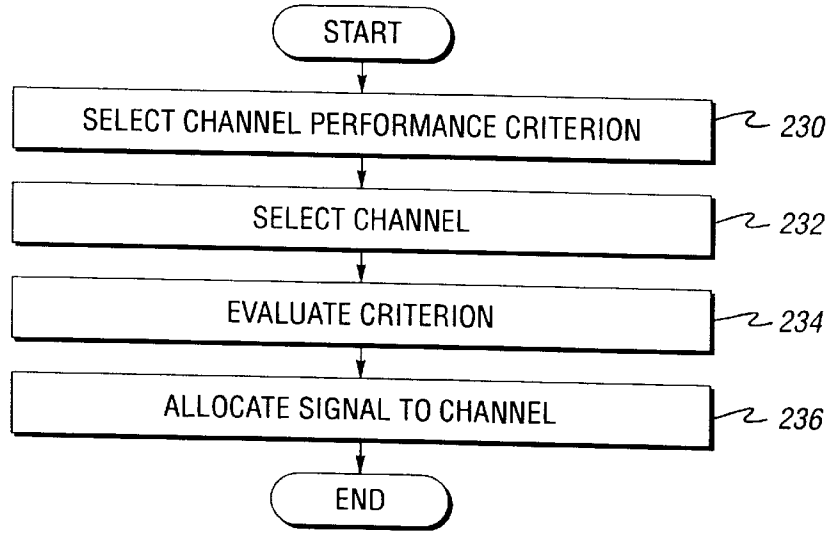


Fig. 8

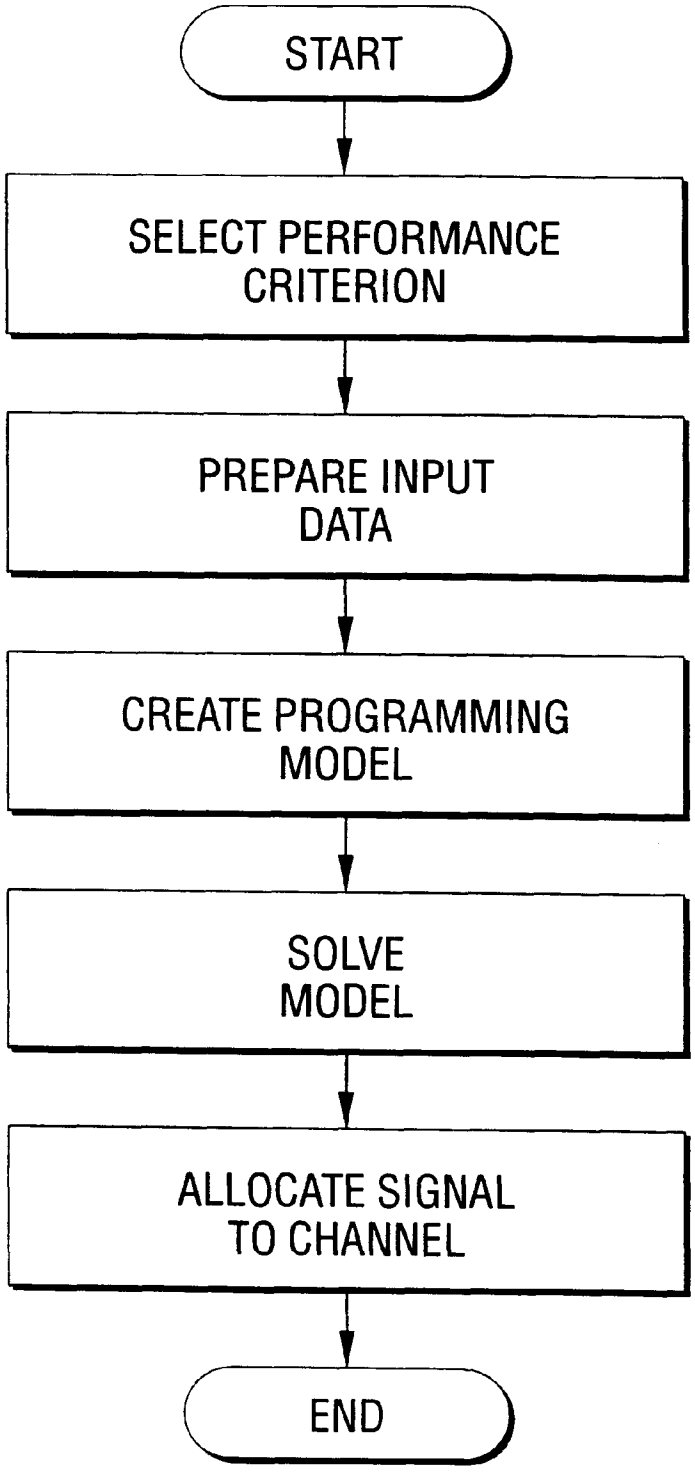

START
SELECT PERFORMANCE CRITERION
PREPARE INPUT DATA
CREATE PROGRAMMING MODEL
SOLVE MODEL
ALLOCATE SIGNAL TO CHANNEL
END

Fig. 9

SIGNAL-TO-CHANNEL MAPPING FOR MULTI-CHANNEL, MULTI-SIGNAL TRANSMISSION SYSTEMS

TECHNICAL FIELD

The present invention relates to a system and method for allocating signal types to transmission channels in a multi-channel, multi-signal transmission system to improve overall system performance.

BACKGROUND ART

Current multi-signal transmission systems deliver multiple types of signals such as telephony, digitized video, and digital data signals over an infrastructure which utilizes various types of physical transmission media. Audio and video information originating at a service provider may be delivered to an end user via a complex switching network employing Radio Frequency (RF), fiber optic, coaxial cable (Coax), and twisted pair copper cabling which may be shielded (STP) or unshielded (UTP). As is known, each type of cabling includes trade-offs between performance characteristics and cost which must be considered in designing and implementing such a transmission system.

As consumers migrate toward information intensive services such as digital television, interactive television, and computer-related on-line services, the demand on the installed infrastructure continues to increase. To meet this increased demand, the physical transmission media forming the delivery infrastructure must eventually be replaced. However, this is an arduous task which requires significant time and expense. Thus, regardless of the particular physical media utilized in any portion of the transmission system, it is desirable to improve the overall system operating performance to maximize or optimize the use of currently installed transmission media.

In a traditional distribution system, a signal which originates at the information service provider may travel through multiple segments of physical transmission media connected by electrical, electronic, or optoelectronic switches before arriving at its destination. The various switches are used to route the signal from a source to a destination where the signals are typically randomly assigned to a particular channel within a multi-channel distribution cable.

SUMMARY OF THE INVENTION

It is thus an object of the present invention to provide a system and method for improving overall system performance in a multi-channel, multi-signal transmission system.

A further object of the present invention is to maximize system performance by selectively assigning particular signal types to particular channels based on a uniform decision rule.

Another object of the present invention is to provide a system and method for optimizing overall system performance by identifying a particular signal-to-channel mapping within a given type of distribution cable which maximizes the minimum margin across all digital links transported by the cable.

A still further object of the present invention is to provide a system and method for communication channel management which utilizes signal-to-noise ratio (SNR) to selectively assign a particular signal to a particular channel based on maximizing the minimum SNR margin across all digital links transported by a particular distribution cable.

Yet another object of the present invention is to provide a system and method for simplifying cable plant recordkeeping by utilizing a consistent decision rule across an entire cable plant region.

In carrying out the above objects and other objects and features of the present invention, a method for allocating a signal to a channel in a multi-channel, multi-signal transmission system is provided. The method includes selecting a channel performance criterion, selecting one of the plurality of channels for evaluation, evaluating the performance criterion for the selected channel for each of the signal types, and allocating a signal type to the selected channel based on the evaluation. A system is also provided for implementing the method of the present invention.

The advantages accruing to the present invention are numerous. For example, the present invention increases system performance for a particular installed transmission system with little or no added cost because the physical transmission media need not be replaced. In addition, the present invention may be quickly implemented since it utilizes the currently installed cable plant. If, on the other hand, new cable plant is to be deployed, application of the present invention maximizes the capabilities of that new cable plant.

The above objects and other objects, features, and advantages of the present invention are readily apparent from the following detailed description of the best mode for carrying out the invention when taken in connection with the accompanying drawings.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. **1** is a block diagram of a broadband transmission architecture from an information service provider to a customer utilizing curbside optical network units (ONUs);

FIG. **2** is a more detailed block diagram of a broadband distribution architecture from a curbside ONU to a particular associated living unit (LU);

FIG. **3** illustrates an alternative broadband transmission architecture from an ONU to an associated LU delivering multiple signal types;

FIG. **4** illustrates filter responses for A-ATM and HSDS CAP-**16** transmitters for random signal-to-channel assignment;

FIG. **5** is a block diagram of a complex baseband receiver equipped with a fractionally spaced linear equalizer and a decision feedback equalizer;

FIG. **6** is a diagram illustrating a particular decision rule in a system and method according to the present invention;

FIG. **7** is a diagrammatic illustration of calculation of crosstalk interference for channel management according to the present invention;

FIG. **8** is a flow chart illustrating a method for channel management according to the present invention; and

FIG. **9** is a flow chart illustrating an alternative implementation of a method for channel management according to the present invention.

BEST MODE FOR CARRYING OUT THE INVENTION

Referring now to FIG. **1**, a block diagram of a multi-channel, multi-signal transmission system architecture is shown. The system, indicated generally by reference numeral **10**, delivers various types of signals, such as telephony, compressed digital video, data, and broadcast video, from an information provider **12** to one or more living units **14**. System **10** is divided into a digital transport

network, indicated generally by reference numeral **16**, in parallel with an analog NTSC broadcast video overlay, indicated generally by reference numeral **18**. The digital portion of the network carries both Asymmetric Asynchronous Transfer Mode (A-ATM) and Synchronous Transfer Mode (STM) traffic over separate Interoffice Facilities and integrated access networks. STM traffic consists of telephony and packet data while A-ATM traffic carries compressed digital video, control channels, and other forms of data. As these types of systems evolve, the transport of broadcast video channels will likely migrate from analog portion **18** to digital portion **16**.

With continuing reference to FIG. **1**, a digital signal originating at information providers **12** may pass through a number of narrowband STM and broadband ATM switches, such as ATM Video Switch **20**, which route the digital traffic to Host Digital Terminals (HDTs) **22** within each serving Central Office **24**. A fiber optic system **26** delivers A-ATM and STM traffic to a set of remote Optical Network Units (ONUs) **28**, each of which routes the correct signals to a set of **16–32** subtending Living Units (LUs) **14**.

Analog signals may be captured by RF receivers at information providers **12** and transmitted to RF modulators **32** within Level 1 gateways **30** where they are converted to optical signals via laser **34**. The optical signals are transmitted via optical fiber **40** to appropriate receivers **36** within each serving Central Office **24**. The signals may be processed and retransmitted by laser **38** over optical fiber **40'** to video nodes **42** where they are converted to electrical signals which are transmitted to splitter amplifiers **46** which distribute the signal via coax **48**. These signals may be delivered directly to a living unit **14** or combined in an ONU **28** as explained in greater detail with reference to FIG. **2**.

Each ONU is capable of providing copper UTP **52** and coax drop lines **54** to a Network Interface Device (NID) **56** of an associated LU **14**. A number of devices may be connected to NID **56**, such as telephones **58**, computers **60**, set-top terminals, i.e. "decoder boxes" **62**, televisions **64**, and the like. Such devices may be generally referred to as Customer Premise Equipment (CPE) **66**.

FIG. **2** illustrates one possible transmission system architecture for distributing signals from a particular ONU **28** to its associated LUs **14** (only one of which is specifically illustrated). As shown, the links between an LU **14** and its associated ONU **28** include a combination of copper twisted pairs **84** and coaxial cabling **92**. Twisted pair distribution cable **82** carries signals between ONU **28** and its subtending downstream pedestals **86** via associated twisted pairs **84**. Allocation of particular signal types to a particular twisted pair within distributing cable **82** according to the present invention may be performed by control logic **80**. Alternatively, channel management according to the present invention may be performed by a programmed microprocessor prior to a hardwired implementation which assigns particular signal types to particular channels across the entire cable plant based on the results generated by the microprocessor.

With continuing reference to FIG. **2**, distribution cable **82** may be an air-core (aerial) or filled (buried) cable having 28, 50, or 84 twisted pairs. Preferably, the length of distribution cable **82** is less than or equal to 600 feet. Twisted pairs **84** within each distribution cable **82** are divided into sets of four, with each set dedicated to a specific LU. Although not specifically illustrated, some installations allow LUs **14** which are in close proximity to an ONU **28** to be served directly by twisted pair and coaxial drop cables without the use of an intervening distribution cable **82**.

The concept of allocating a set of twisted pairs **84** for each LU **14**, with each set to be used only for connecting to its intended LU and never any of the other LUs, is referred to as a dedicated plant. Use of dedicated cable plant according to the present invention simplifies the recordkeeping for channel management as described in greater detail below.

In one embodiment, three of the twisted pairs **84** within distribution cable **82**, referred to as the narrowband pairs, are utilized for delivery of narrowband telephony services such as POTS (Plain Old Telephone Service), ISDN (Integrated Services Digital Network) basic rate, or low speed data services. By utilizing the system and method of the present invention, these narrowband pairs may be utilized more efficiently. A fourth twisted pair **84** within each set, referred to as the A-ATM pair, carries A-ATM digital video and/or data in the downstream direction (from the service provider toward the customer), and signalling, control, and digital data in the upstream direction (from the customer toward the service provider).

The downstream signal within each A-ATM pair carries ATM cells embedded in the payload of a SONET STS-1 (51.84 Mb/s) physical frame, using a 16-point Carrierless Amplitude/Phase (CAP-16) line code, well known in the art. The upstream signal in an A-ATM pair also carries ATM cells, but at a reduced line rate of 1.62 Mb/s using a CAP-4 line code. Simultaneous upstream and downstream transport over each A-ATM pair is provided through frequency division multiplexing of the two signals.

As illustrated in FIG. **2**, the STM signals are transmitted from pedestal **86** to an NID **56** using a UTP drop cable **90**. From NID **56**, existing in-home wiring carries these signals to various CPE devices **66**. The A-ATM pair terminates at the pedestal **86** on a Video Signal Combiner (VSC) **88** within pedestal **86**. The VSC combines the video signal from the A-ATM pair with the analog video signal coming in from the distribution coax cable **54**. Because the A-ATM and analog video signals are spectrally separated (analog NTSC video signals start at 54 MHz), they can be carried together to NID **56** on a single RG-6 drop coax **92**. Transport of these signals from NID **56** to terminals **60***a* is via the existing in-home splitter **94** and coax bus **96** within LU **14**.

Preferably, the UTP drop cable **90** has a cable length from pedestal **86** to NID **56** of less than or equal to 200 feet. Also preferably, in-home wiring within each LU **14** has a cable length of less than or equal to 100 feet.

During times of high demand, a given ONU **28** transmits and receives A-ATM signals to and from multiple subtending LUs simultaneously. During such times, the CAP-16 downstream signals on the separate A-ATM cable pairs will interfere with one another through an electromagnetic coupling mechanism known as Far End Crosstalk (FEXT). Upstream CAP-4 signals simultaneously present on separate pairs will similarly generate and be exposed to FEXT interference. The signals may also introduce Near End Crosstalk (NEXT) interference to the transport system, which is even more debilitating than FEXT.

As network traffic continues to increase, and additional High-Speed Symmetric Data Services (HSDS) are added, it becomes more difficult to maintain an acceptable transport margin for a target Bit Error Rate (BER), for example a design margin of 6 dB at 10^{-9} BER. This is due to the effects of NEXT, FEXT, electromagnetic interference (EMI), impulse noise, temperature effects, and the like. As explained below, a channel management strategy according to the present invention improves the overall transmission system performance as measured by the ability to achieve a

particular target BER or signal-to-noise ratio (SNR) at an acceptable margin, or other such performance criterion.

One approach to improving transmission system performance is to replace the telephony exchange distribution cable with cables having better characteristics for attenuation, NEXT, FEXT, and the like. Cross-talk performance may be improved by using tighter twist rates on twisted pair cabling. In addition, proper shielding helps to eliminate EMI. However, the present invention may be utilized separately from, or in addition to, replacing existing exchange cabling to improve overall system performance. As such, implementation of the present invention provides interim performance increases almost immediately while awaiting available resources to replace the existing cable plant.

Referring now to FIG. **3**, a block diagram illustrating one possible construction of an information distribution system according to the present invention is shown. The system combines an improved distribution cable **82'** and channel management performed by control logic **80'** with an ONU **28'** to improve overall system performance. As previously described, control logic may reside within each ONU or, preferably is executed prior to installation of the cable plant (or portion thereof) so that each ONU may be hardwired based on the result of the signal-to-channel optimization.

The system of FIG. **3** could be used to simultaneously deliver telephony, A-ATM, and HSDS services to customers. In this example, ONU **28'** serves a total of 16 LUs, such as LU **14'**. Of the 16 LUs, 12 LUs are served by a 50-pair distribution cable **82'** and a collection of drop cables, indicated generally by reference numeral **116**. Preferably, distribution cable **82'** has a cable length less than or equal to 600 feet while drop cables **116** have a cable length of less than or equal to 200 feet from pedestal **86'** to their corresponding LUs. The remaining four LUs served by ONU **28'** are served directly over a similar set of drop cables **108** and **110**. As with the system illustrated in FIG. **2**, the system of FIG. **3** allocates four twisted pairs for each LU such that all LUs could be simultaneously served with A-ATM, HSDS, and POTS services.

The ONU **28'** includes a set of 16 A-ATM downstream transmitter and upstream receivers **100**. To provide HSDS, 16 downstream transmitters **102** and upstream receivers **104** may also be provided in addition to a set of 16 narrowband telephony cards **106**. HSDS transmitters and receivers **102** and **104** may optionally process narrowband signals as well, or interface with existing narrowband cards. ONU **28'** also includes control logic **80'** which may be used implement channel management according to the present invention.

As stated herein, the use of dedicated plant allocates four twisted pairs **84'** within distribution cable **82'** for access to a given LU, such as LU **14'**. One of the four twisted pairs carries an A-ATM signal to pedestal **86'** where the A-ATM signal is combined by VSC **88'** with an analog video signal (not specifically illustrated). The combined signal, which is frequency division multiplexed, is carried to the LU on a single coax drop cable **122**. The second of the four twisted pairs carries narrowband telephony to pedestal **86'** with a telephony drop **119** completing the connection to the NID **56'**. The third and fourth twisted pairs carry upstream and downstream HSDS signals, respectively, to pedestal **86'** and then to NID **56'** via UTP drop cable **118**, which preferably meets the requirements of a category 5 cable as rated by the Electronics Industry Association/Telephone Industry Association (EIA/TIA). Where a CAP-type signaling scheme is utilized for HSDS signals, the third and fourth twisted pairs can optionally simultaneously transport narrowband and HSDS signals so that an LU requesting HSDS would not be limited to a single narrowband channel. This type of simultaneous single pair narrowband and HSDS transport may be accomplished through the use of POTS splitting filters within NID **116**.

Within an LU **14'**, existing coaxial cable **96'** and twisted pair **113** is used for A-ATM and narrowband in-home transport. An HSDS may require a category 5 cable **114** with a cable length of less than or equal to 100 feet to connect the POTS splitter and a network port **112** of the corresponding HSDS CPE.

Thus, FIG. **3** illustrates four different types of digital transmission links, each of which may contribute transmission impairments to the system. Such impairments include, but are not limited to, NEXT, FEXT, and Additive White Gaussian Noise (AWGN). Since the A-ATM upstream link operates within the 28–30 MHz band, the introduction of HSDS signals, which preferably utilize CAP-16 coding operating in the 0.5–26 MHz band, does not adversely impact this link.

The A-ATM downstream link from transmitter **100** operates in the 6–26 MHz band while both upstream and downstream CAP-16 HSDS links to transmitters **102** and receivers **104** operate in the 1–26 MHz region. As a result, the A-ATM downstream receiver within LU **14'** must operate acceptably subject to the following impairments: FEXT from up to 11 A-ATM transmitters in the same distribution cable; FEXT from up to 12 HSDS downstream transmitters; NEXT from up to 12 HSDS upstream transmitters; and AWGN.

The introduction of HSDS signals into distribution cable **82'** generates new NEXT and FEXT impairments with which the A-ATM receivers **112** must contend. The NEXT from the upstream HSDS transmitters is of special concern because NEXT is more troublesome to the transmission than FEXT. Where the distribution cable specification describes bounds on worst-case FEXT power sum, it is useful for system simulation purposes to replace the two types of FEXT disturbers with one, while keeping the total number of interfering transmitters constant. The worst-case performance of the actual dual-source FEXT configuration will then lie between that of the two single-source FEXT cases.

The HSDS upstream link to receiver **104** must operate in the presence of the following impairments: NEXT from up to 12 HSDS downstream transmitters; NEXT from up to 12 A-ATM downstream transmitters; FEXT from up to 11 other HSDS upstream transmitters; and AWGN. Again, the worst-case performance will lie between that of systems with 11 HSDS FEXT, AWGN, and NEXT from either 24 HSDS or 24 A-ATM downstream transmitters.

The HSDS CAP-16 downstream link from transmitter **102** must operate in the presence of the following impairments: NEXT from the single co-located HSDS upstream transmitter; NEXT from up to 11 other HSDS upstream transmitters; FEXT from up to 11 other HSDS downstream transmitters; FEXT from up to 12 A-ATM downstream transmitters; and AWGN.

Computer simulations of the various links in the transport system of FIG. **3** have been utilized to determine worst-case margin at a particular target BER. These results indicate a significant improvement in overall system performance when utilizing a channel management strategy according to the present invention compared to the traditional random assignment for the various upstream and downstream signal types. In one embodiment, the goal is to improve the

worst-case performance of the limiting link by intelligently mapping channels, or twisted pairs within a distribution cable, to a particular signal type. Preferably, a single decision rule based on predetermined cable characteristics is applied uniformly across all ONU installations. In this case, the worst-case margin for a link is the minimum margin experienced across all pairs assigned to that link type.

FIG. **4** illustrates the response characteristics for filters used in a simulation of the transmission system of FIG. **3**. As illustrated, the HSDS filter response **122** extends from about 0.5 MHz to about 26 MHz while the A-ATM filter response **120** extends from about 6 MHz to about 26 MHz. For the simulation, receiver AWGN included amplifier thermal noise at −130 dBm/Hz in addition to quantization noise introduced by an 8-bit A/D. All subtending pedestals from the ONU being simulated were assumed to be 600 feet away from that ONU. While in actual implementations the pairs for consecutive sets of four LUs may be spliced at pedestals every 100–200 feet along the distribution, the level of NEXT, which is the dominant impairment in the links under study, will not be appreciably affected by that assumption.

For simulations of the HSDS upstream link, the LU drop cables were assumed to be approximately 200 foot in length with an additional 100 feet of wiring length within the LU. For simulations of the downstream A-ATM link, the LU housing the receiver under study was assumed to be 900 cable-feet away from the ONU. In an attempt to reasonably maximize that link's NEXT level, however, the other LU upstream transmitters were only 50 cable feet away from the downstream distribution cable end. The results were based on a CAP-16 adaptive receiver model with 32 fractionally spaced equalizer taps (T/4) and a decision feedback equalizer as illustrated and described with reference to FIG. **5**.

Referring now to FIG. **5**, the simulation assumed the complex fractionally-spaced linear equalizer (FSE) **124** contains taps **126**, represented by f_k where $-L \leqq k \leqq M$ with L taps before and M taps after a reference tap f_0 (not specifically illustrated), and that for a symbol period of T, the tap spacing is pT/q for positive integers p and q as indicated by reference numeral **128**. The decision feedback equalizer (DFE) **130** contained N taps **132**, represented by d_k where $1 \leqq k \leqq N$ and where N may be zero indicating that the decision feedback equalizer loop is not present. The complex baseband input signal s(t) may be represented by:

$$s(t) = \sum_{i=0}^{I} \left\{ \sum_{n} a_n^i h_i(t - nT) \right\} + v(t) \tag{1}$$

where a_n^0 is the symbol sequence to be detected, a_n^i, $1 \leqq i \leqq I$, are the symbol sequences carried by I synchronous interfering signals, $h_0(t)$ is the main channel complex equivalent baseband impulse response, and $h_i(t)$, $1 \leqq i \leqq I$, are the interfering channel complex equivalent baseband impulse responses. v(t) is colored Gaussian noise with the sampled autocorrelation sequence:

$$\eta_k = \frac{1}{A^2} E[v(t + kpT/q)v^*(t)] \tag{2}$$

where the symbol sequences are assumed white and of power A^2, i.e.,

$$E[a_n^i (a_{n-k}^j)^*] = A^2 \delta_k \delta_{i-j},\ 0 \leqq i \leqq I,\ 0 \leqq j \leqq I \tag{3}$$

Then define the vector and matrix quantities,

$$f = [f_{-L} f_{-L+1} \ldots f_M]^T \tag{4}$$

$$d = [d_1 d_2 \ldots d_N]^T \tag{5}$$

$$h = [h_0(LpT/q) h_0([L-1]pT/q \ldots h_0(-MpT/q)]^T \tag{6}$$

$$H = \begin{bmatrix} h_0*(1+Lp/q]T) & h_0^*([1+(L-1)p/q]T & \ldots & h_0^*([1-Mp/q]T) \\ h_0^*([2+Lp/q]T) & h_0^*([2+(L-1)p/q]T) & \ldots & h_0^*([2-Mp/q]T) \\ h_0^*([N+Lp/q]T) & h_0^*([N+(L-1)p/q]T & \ldots & h_0^*([N-Mp/q]T) \end{bmatrix} \tag{7}$$

and

$$R = [r(i,j), -L \leqq i,j \leqq M] \tag{8}$$

where

$$r(i,j) = \eta_{j-i} + \sum_{m \notin [1,N]} h_0([m - ip/q]T) h_0^*([m - jp/q]T) + \sum_{k=1}^{I} \sum_{m} h_k([m - ip/q]T) h_k^*([m - jp/q]T) \tag{9}$$

and where $(\ )^T$ denotes matrix transpose. With these definitions, the MMSE FSE and DFE taps are given by:

$$f_{opt} = (R^{-1}h)^* \tag{10}$$

$$d_{opt} = H^* f_{opt} \tag{11}$$

and the MMSE is:

$$j_{min} = A^2(1 - h^H R^{-1} h) \tag{12}$$

where $(\ )^H$ denotes conjugate transpose. For a QAM16 or CAP-16 constellation, $A^2 = 10$, and the receiver symbol error rate is:

$$Pr(\text{error}) = 3Q\left(\sqrt{2/J_{\min}}\right) \tag{13}$$

where

$$Q(x) = \frac{1}{\sqrt{2\pi}} \int_x^\infty e^{-y^2/2} dy \cong \frac{e^{-x^2/2}}{x\sqrt{2\pi}} \tag{14}$$

The results of the simulations reflected the evaluation of Equations 10–14 for particular channel and noise conditions. The channel in all cases consisted of the cascade of the insertion gain of 600 feet of distribution cable, the appropriate drop in inside wiring cables, and the transmit filter shown in FIG. **4**. The colored Gaussian noise consists of AWGN plus any stationary NEXT or FEXT sources, the power spectral densities of which are given by:

$$S_{NEXT}(f) = cf^{3/2} S_{TX}(f) \tag{15}$$

and

$$S_{FEXT}(f) = Klf^2 S_{TX}(f) |H_{cable}(f)|^2 \tag{16}$$

where $S_{TX}(f)$ is the disturbing transmitters' power spectral density, $H_{cable}(f)$ is the disturbing cable's frequency response, and for 1 in feet and f in Hertz the constants C and K are given in Table 1, at zero dB margin noise levels.

TABLE 1

NEXT and FEXT Coupling Constants For Different Cable Types

Cable Type	C(0 dB Margin)	K (0 dB Margin)
50-Pair Exchange	8.817×10^{-14}	8.001×10^{-20}
Shielded EIA/TIA Category 4	2.336×10^{-15}	8.106×10^{-21}
EIA/TIA Category 5	5.869×10^{-16}	NA

The determination of a link's margin is made by scaling all 0 dB noise and interference powers by an amount corresponding to the margin, and recording the resulting BER from Equation (13). The margin at which the target BER is recorded is, by definition, the margin of the link.

Applying this analysis to the transmission system links illustrated and described with reference to FIG. **3** results in the following worst-case results summarized in Table 2.

TABLE 2

Worst-Case Simulated Link Margins With Random Pair-to-Signal Mappings

Link	Impairments	Worst-Case Margin
HSDS Upstream 51.84 Mb/s	• Power-Sum Spec NEXT from HSDS downstream TX • Power-Sum Spec FEXT from HSDS upstream TX • AWGN (−130 dBm/Hz plus 8-bit A/D)	1.0 dB
HSDS Upstream 51.84 Mb/s	• Power-Sum Spec NEXT from A-ATM downstream TX • Power-Sum Spec FEXT from HSDS upstream TX • AWGN (−130 dBm/Hz plus 8-bit A/D)	1.8 dB
A-ATM Downstream 51.84 Mb/s	• Power-Sum Spec NEXT from HSDS upstream TX • Power-Sum Spec FEXT from A-ATM downstream TX • AWGN (−130 dBm/Hz plus 8-bit A/D)	2.0 dB
A-ATM Downstream 51.84 Mb/s	• Power-Sum Spec NEXT from HSDS upstream TX • Power-Sum Spec FEXT from HSDS downstream TX • AWGN (−130 dBm/Hz plus 8-bit A/D	2.3 dB

As can be seen, the HSDS upstream link is limiting for the random pair mapping case, i.e. where no channel management strategy is utilized. Neither the HSDS upstream nor the A-ATM downstream links appeared to meet a target performance level of 6.0 dB margin with a 10^{-9} BER. Regardless of the particular target margins, or other performance criterion, channel management according to the present invention improves system robustness against NEXT and FeXT with no increase in capital costs associated with cable plant replacement. For any particular transport system, such as that illustrated in FIG. **3**, an improvement of approximately 10 dB margin is expected.

A system and method for multi-signal, multi-channel management according to the present invention will now be described with reference to FIGS. **6–8**. One embodiment of a channel management strategy is illustrated schematically in FIG. **6**. ONU **130** is connected to a pedestal (not specifically illustrated) by a number of twisted pairs within a distribution cable **140**. The twisted pairs are arranged in a number of binder groups, such as binder group **134** or binder group **138**, which are physically separated from each other within distribution cable **140**. The various binder groups may be logically divided (i.e. not actually separated) into two equally sized sets, such as downstream set **132** and upstream set **136**. Each downstream binder group set **132** would include 1 A-ATM and 1 HSDS downstream twisted pair per LU. Each upstream binder group set **136** would include one HSDS upstream pair and one POTS only pair per LU.

Control logic **150** within ONU **130** may be used to implement a particular channel management strategy according to the present invention. As disclosed above, the present invention contemplates a fixed mapping of each LU signal to a specific distribution cable pair where the same mapping is applied consistently to all ONUs. Table 3 illustrates the results of an example decision rule in a channel management strategy for an ONU with 16 subtending LUs. A 50-pair distribution cable serves 12 of the 16 LUs, and 4 LUs are served directly via drop cables as illustrated in FIG. **3**.

TABLE 3

Example Pair Management Rule in a 50-Pair Buried Cable

LU	SIGNALS	BINDER GROUP	Pairs
1	A-ATM, HSDS Downstream	Blue-White	1, 2
1	HSDS Upstream, POTS	Orange-White	1, 2
2	A-ATM, HSDS Downstream	Blue-White	3, 4
2	HSDS Upstream, POTS	Orange-White	3, 4
3	A-ATM, HSDS Downstream	Blue-White	5, 6
3	HSDS Upstream, POTS	Orange-White	5, 6
.	.	.	.
.	.	.	.
.	.	.	.
12	A-ATM, HSDS Downstream	Blue-White	23, 24
12	HSDS Upstream, POTS	Orange-White	23, 24

The correspondence between a given residence and its LU number as shown in Table 3 may be arbitrary or more may be established according to certain other decision rules. For the example decision rule illustrated in Table 3, after LU number 1 is identified, all that is required is that pair 2 from the blue-white binder group be allocated for HSDS downstream transport to that LU. Similarly, pair one from the blue-white group is reserved for A-ATM. In a like manner, every other cable pair is reserved for the transport of a certain signal type (A-ATM, POTS, HSDS downstream, or HSDS upstream) to a certain LU number. In addition to improving the overall performance of the transport system, implementation of a channel management scheme according to the present invention simplifies recordkeeping and associated aspects of network operations.

For example, the only information required to identify the channel belonging to the residence at 123 Main Street is a record of the fact that, within its ONU neighborhood, 123 Main Street is LU No. 7.

Preferably, channel management according to the present invention identifies the channel-to-signal mapping within a given distribution cable type (i.e. buried or aerial) that maximizes or optimizes the overall system performance based on one or more predetermined criterion. For each possible channel-to-signal mapping, the NEXT and FEXT

power sums as a function of frequency are determined based on measured channel-to-channel responses. This information may then be used to evaluate the criterion, such as transport margin or SNR, for each of the digital links within a particular distribution cable. The particular mapping which results in maximizing or optimizing the selected criterion is then used to assign a particular signal type to each of the channels within the distribution cable.

Referring now to FIG. **7**, a formulation of the optimization problem for a multiple twisted pair distribution cable is illustrated diagrammatically. The distribution cable connects downstream transmitters **200**,**212** to receivers **208**, **216** and upstream transmitters **206**,**218** to receivers **202**, **210**, respectively, via twisted pairs **204**,**214**. M represents a set of copper pairs within a distribution cable, indexed by i where i ranges from unity to n, the total number of copper pairs in a cable. M represents a set of signal types carried over the distribution cable, indexed by k which ranges from unity to m where each signal type implies a specific upstream and downstream signal (e.g. where signal one is A-ATM, signal two is HSDS downstream, signal three is HSDS upstream, and signal four is a POTS only signal). Thus, m_k represents the number of signals of type kϵM to be carried in the cable.

With continuing reference to FIG. **7**, $N_{i,j,t}{}^{u}$ represents the NEXT from pair i **204** into pair j **214** upstream receiver **210** at frequency sample of tϵT, indicated generally by reference numeral **220**. Similarly, reference numeral **226** indicates the NEXT as represented by $N_{i,j,t}{}^{d}$, from pair i **204** into pair j **214** downstream receiver **216** at frequency sample tϵT. Likewise, reference numeral **224** indicates FEXT, represented by $F_{i,j,t}{}^{u}$, from pair i **204** into pair j **214** upstream receiver **210** at frequency sample tϵT while reference numeral **222** indicates FEXT, represented by $F_{i,j,t}{}^{d}$ from pair i **204** into pair j **214** downstream receiver **216** at frequency sample tϵT.

The total power received by downstream receiver **208** on pair i **204** is given by:

$$S_i^d = \sum_{t\in T} S_{i,t}^d \tag{17}$$

where $S_i{}^{d}$ is the total received power, $S_{i,t}{}^{d}$ is the signal power into receiver **208** at frequency sample tϵT. Similarly, the total power received by receiver **202** on pair i **204** may be represented by:

$$S_i^u = \sum_{t\in T} S_{i,t}^u \tag{18}$$

where $S_i{}^{u}$ represents the total received power and $S_{i,t}{}^{u}$ represents the signal power into receiver **202** at frequency sample tϵT.

The total power contributed by NEXT and FEXT into upstream receiver **202** on pair i **204** may be represented by:

$$Q_i^u = \sum_{t\in T} Q_{i,t}^u, \tag{19}$$

and likewise, the total power contributed by NEXT and FEXT into downstream receiver **208** on pair i **204** may be represented by:

$$Q_i^d = \sum_{t\in T} Q_{i,t}^d, \tag{20}$$

where:

$Q_{i,t}{}^{d}$ represents the NEXT and FEXT power into downstream receiver **208** on pair i **204** at frequency sample tϵT;

$Q_{i,t}{}^{u}$ represents NEXT and FEXT power into upstream receiver **202** on pair i **204** at frequency sample tϵT;

$Q_i{}^{u}$ represents the total NEXT and FEXT power into upstream receiver **202**; and

$Q_i{}^{d}$ represents the total NEXT and FEXT power into downstream receiver **208**.

The total noise power, $V_i{}^{d}$, from sources other than NEXT and FEXT into downstream receiver **208** on pair i **204** may be represented by:

$$V_i^d = \sum_{t\in T} V_{i,t}^d, \tag{21}$$

where $V_{i,t}{}^{d}$ represents noise power from sources other than NEXT and FEXT into downstream receiver **208** at frequency sample t. Similarly, the total noise power, $V_i{}^{u}$, from sources other than NEXT and FEXT coupled into upstream receiver **202** may be represented by:

$$V_i^u = \sum_{t\in T} V_{i,t}^u \tag{22}$$

where $V_{i,t}{}^{u}$ is the noise power from sources other than NEXT and FEXT, into receiver **202** at frequency sample t.

If χ_{ik}=1, when pair iϵN carries signal type kϵM and χ_{ik}=0 otherwise, then, for each iϵN and tϵ T, $S_{i,t}$, $Q_{i,k}$, $V_{i,t}$ and G_i can be represented as follows:

$$S_{i,t}^d = |F_{i,i,t}^d|^2 \sum_{k\in M} P_{k,t}^d \chi_{i,k}, \tag{23}$$

$$S_{i,t}^u = |F_{i,i,t}^u|^2 \sum_{k\in M} P_{k,t}^u \chi_{i,k}, \tag{24}$$

$$Q_{i,t}^d = \sum_{j\in N, j\neq i} \sum_{k\in M} \chi_{jk}\left(P_{k,t}^d |F_{j,i,t}^d|^2 + P_{k,t}^u |N_{j,i,t}^d|^2\right) \tag{25}$$

$$Q_{i,t}^u = \sum_{j\in N, j\neq i} \sum_{k\in M} \chi_{jk}(P_{k,t}^u |F_{j,i,t}^u|^2 + P_{k,t}^d |N_{j,i,t}^u|^2) \tag{26}$$

$$V_{i,t}^u = \sum_{k\in M} \chi_{ik} W_{k,t}^u \tag{27}$$

$$V_{i,t}^d = \sum_{k\in M} \chi_{ik} W_{k,t}^d \tag{28}$$

$$G_i^d = \sum_{k\in M} \chi_{ik} H_k^d \tag{29}$$

$$G_i^u = \sum_{k\in M} \chi_{ik} H_k^u \tag{30}$$

where:

$W_{k,t}{}^{d}$ is noise power from sources other than NEXT and FEXT into a downstream receiver of signal type k at frequency sample tϵT;

$W_{k,t}^{u}$ is noise power from sources other than NEXT and FEXT into an upstream receiver of signal type k at frequency sample t∈T;

G_i^u=SNR reference level for upstream receiver on pair i ∈N;

G_i^d=SNR reference level for downstream receiver on pair i∈N;

H_d^k is the SNR reference level for downstream receiver of signal type k∈M;

H_u^k is the SNR reference level for upstream receiver of signal type k∈M;

$P_{k,t}^{u}$=power spectral density (PSD) of signal type k, upstream channel, at frequency sample t∈T; $P_{k,t}^{d}$= power spectral density (PSD) of signal type k, downstream channel, at frequency sample t∈T.

The optimal pair assignment problem based on maximizing the minimum SNR margin, measured relative to given SNR references $\{G_i^u, G_i^d\}$, can be formulated as follows:

$$\text{Maximize } \min_{i\in N}\left\{\min\left(\frac{S_i^d}{(Q_i^d+V_i^d)G_i^d}, \frac{S_i^u}{(Q_i^u+V_i^u)G_i^u}\right)\right\} \quad (31)$$

subject to

$$\sum_{i\in N}\chi_{ik} = m_k \qquad \forall\, k\in M \quad (32)$$

$$\sum_{k\in M}\chi_{ik} = 1 \qquad \forall\, i\in N \quad (33)$$

$$\chi_{ik}\in\{0,1\}, \qquad \forall\, i\in N, \forall\, k\in M.$$

Referring now to FIG. **8**, a flow chart illustrating a method of channel management according to the present invention is shown. As will be appreciated by one of ordinary skill in the art, the method may be performed by control logic implemented by software in conjunction with a programmable microprocessor, hardware, or a combination of both. Hardware may include dedicated electrical and electronic circuits, or programmable devices such as FPGAs and the like.

As represented by block **230** of FIG. **8**, one or more channel performance criterion are selected based on the particular application. Performance criterion may be SNR, BER, margin, and the like since the present invention is not limited to a particular criterion but utilizes one or more rules of decision to allocate signals to channels.

Block **232** of FIG. **8** represents selecting a particular channel mapping which allocates a signal type to each available channel. The performance criterion selected in step **230** is then evaluated for the particular signal-to-channel mapping, selected at step **232**, as represented by step **234**. Steps **232** and **234** may be repeated for all of the available signal-to-channel mappings. This may consist of all permutations of signal types and channels, or some subset thereof. Conceptually, steps **232** and **234** represent optimization of the signal-to-channel mapping determined by the performance criterion of step **230** within the operating constraints of the system. Step **236** then allocates a particular signal type to a particular channel within a distribution cable based on the results of the previous steps.

Alternatively, well known mathematical programming algorithms may be used to determine the optimal signal to channel mapping **236**, without the need of repeating steps **232,234** for all possible mappings. A flowchart for one such algorithm described by equations 17–33 is shown in FIG. **9**.

Other techniques also exist which may be used to provide a solution to the multi-signal, multi-channel problem of the present invention.

Referring now to FIG. **9**, a flowchart illustrating an alternative implementation of a method for channel management according to the present invention is shown. Similar to the flowchart of FIG. **8**, block **250** represents selection of a performance criterion for allocating a particular signal type to a particular channel. As described, suitable performance criteria may include any one or a combination of SNR, SNR margin, or the like. Block **252** represents preparation of the input data corresponding to the particular signal types and available channels of a particular application. An instance of an integer programming model is then created based on the input data as represented by block **254**.

With continuing reference to FIG. **9**, the programming model is solved as represented by block **256**. This step includes additional preprocessing of the data to eliminate redundant constraints and variables. Block **256** also includes determining a lower bound by solving the linear programming relaxation and upper bounding by developing a heuristic solution using the genetic algorithm. The steps of lower bounding and upper bounding are then repeated until a gap between the lower and upper bounds satisfies a predetermined error selected based on the particular application. Block **256** then returns a solution which is used to allocate the various signal types to appropriate channels as represented by block **258**.

As previously described, the present invention contemplates implementation of the decision rules across each ONU within the transmission system, thereby simplifying cable plant recordkeeping.

While the best mode for carrying out the invention has been described in detail, those familiar with the art to which this invention relates will recognize various alternative designs and embodiments for practicing the invention as defined by the following claims.

What is claimed is:

1. A method for improving performance of a transmission system used for communicating a plurality of signal types over a plurality of communication channels extending between at least one transmitter and at least one receiver, the method comprising:

selecting at least one performance criterion indicative of signal quality at the at least one receiver;

associating each of the plurality of signal types with a corresponding one of the plurality of communication channels so as to define a plurality of available signal-to-channel maps;

evaluating the selected criterion for each of the plurality of associated signal types and communication channels in a particular signal-to-channel map;

storing a lowest value of the selection criterion for the particular signal-to-channel map;

repeating the steps of evaluating and identifying for each of the plurality of available signal-to-channel maps; and

selecting the signal-to-channel map based on the stored values.

2. The method of claim **1** further comprising:

transmitting each of the plurality of signal types over a corresponding assigned communication channel.

3. The method of claim **1** wherein the step of selecting comprises selecting signal to noise ratio as the at least one performance criterion.

4. The method of claim **1** wherein the step of selecting comprises selecting signal to noise ratio margin relative to a

set of signal to noise ratio references corresponding to the set of signal types as the at least one performance criterion.

5. The method of claim **1** wherein the plurality of signal types includes a digital signal type and wherein the step of selecting includes selecting transmission margin at a predetermined bit error rate as the at least one performance criterion.

6. The method of claim **1** wherein the step of selecting the signal-to-channel map comprises selecting the signal-to-channel map having the highest stored value.

7. The method of claim **1** wherein the step of selecting comprises selecting at least one performance criterion indicative of near-end crosstalk and far-end crosstalk.

8. A method for improving performance of a transmission system used for communicating a plurality of signal types over a distribution cable having a plurality of twisted pairs extending between at least one transmitter and at least one receiver, the method comprising:

associating each of the plurality of signal types with a corresponding one of the plurality of twisted pairs so as to define a plurality of available signal-to-pair mappings;

measuring pair to pair electromagnetic coupling for at least two of the plurality of twisted pairs;

selecting the signal-to-lair mapping which improves system performance as determined by the measured pair to pair electromagnetic coupling; and

assigning each of the plurality of signal types to one of the plurality of twisted pairs based on the selected signal-to-pair mapping.

9. The method of claim **8** further comprising:

transmitting each of the plurality of signal types over a corresponding assigned twisted pair.

10. The method of claim **9** wherein the plurality of twisted pairs is separated into a plurality of binder groups, the plurality of signal types includes an upstream signal traveling in a direction opposite to a downstream signal, and wherein the step of assigning comprises:

assigning the upstream signal to a first one of the plurality of binder groups and assigning the downstream signal to a second one of the plurality of binder groups.

11. The method of claim **10** wherein the upstream and downstream signals are digital signals.

12. The method of claim **8** wherein the plurality of signal types includes at least one digital signal and wherein the step of measuring comprises:

computing the near end crosstalk and far end crosstalk power sums as a function of frequency; and

computing transmission margin for each of the at least one digital signal types for a predetermined error rate.

13. The method of claim **12** wherein the step of assigning comprises assigning each of the plurality of signal types to one of the plurality of twisted pairs based on the signal-to-pair mapping which maximizes the minimum transmission margin at a predetermined bit error rate.

14. The method of claim **12** wherein the step of assigning comprises assigning each of the plurality of signal types to one of the plurality of twisted pairs based on the signal-to-pair mapping which optimizes signal to noise margin.

15. The method of claim **12** wherein the step of assigning comprises assigning each of the plurality of signal types to one of the plurality of twisted pairs based on the signal-to-pair mapping which optimizes signal to noise ratio.

16. Apparatus for improving performance of a transmission system used for communicating a plurality of signal types over a plurality of communication channels extending between at least one transmitter and at least one receiver, the apparatus comprising:

control logic for selecting at least one performance criterion indicative of signal quality at the at least one receiver, evaluating at least one rule of decision based on the at least one performance criterion,

associating each of the plurality of signal types with a corresponding one of the plurality of communication channels so as to define a plurality of available signal-to-channel maps,

evaluating the selected criterion for each of the plurality of associated signal types and communication channels in a particular signal-to-channel map,

storing a lowest value of the selection criterion for the particular signal-to-channel map,

repeating the steps of evaluating and identifying for each of the plurality of available signal-to-channel maps,

selecting the signal-to-channel map based on the stored values.

17. The apparatus of claim **16** wherein the control logic selects the signal-to-channel map having the highest stored value.

18. The apparatus of claim **16** wherein the control logic selects signal-to-noise ratio margin as the at least one performance criterion.

19. The apparatus of claim **16** wherein the control logic evaluates at least one rule of decision based on mathematical optimization which maximizes a minimum value of the at least one performance criterion.

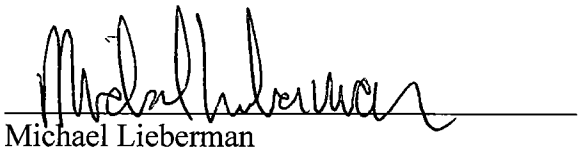
* * * * *

CERTIFICATE OF SERVICE

I hereby certify that on June 6, 2012, I caused a true and correct copy of the foregoing Amended Complaint and Supplemental 7.1 Statement to be served via First Class Mail, postage prepaid, and E-mail upon the following:

Howard M. Klein
Andrew S. Gallinaro
Conrad O'Brien
1500 Market St Suite 3900
Centre Square West Tower
Philadelphia, PA 19102-2100
hklein@conradobrien.com
agallinaro@conradobrien.com

ATTORNEYS FOR SPRINT COMMUNICATIONS COMPANY L.P., SPRINT SPECTRUM L.P., AND NEXTEL OPERATIONS, INC.



Michael Lieberman